Kerio WinRoute Firewall 6™

Administrator's Guide

Kerio Technologies

© Kerio Technologies. All Rights Reserved.

Release Date: March 14, 2007

This guide provides detailed description on the *Kerio WinRoute Firewall*, version *6.3.0*. All additional modifications and updates reserved.

For current product version, check http://www.kerio.com/kwfdwn.

Information regarding registered trademarks and trademarks are provided in attachment A.

Contents

1 Quick Checklist 8

2 Introduction 10
2.1 Kerio WinRoute Firewall 10
2.2 Conflicting software 13
2.3 Installation 15
2.4 WinRoute Components 20
2.5 WinRoute Engine Monitor 21
2.6 Upgrade and Uninstallation 22
2.7 Configuration Wizard 24

3 WinRoute Administration 27
3.1 Administration Window 27
3.2 View Settings 30

4 Product Registration and Licensing 32
4.1 License types and number of users 32
4.2 License information 34
4.3 Registration of the product in the Administration Console 36
4.4 Product registration at the website 44
4.5 Subscription / Update Expiration 44
4.6 User counter 46

5 Settings for Interfaces and Network Services 49
5.1 Network interfaces 49
5.2 Connection Failover 56
5.3 DNS Forwarder 60
5.4 DHCP server 66
5.5 Proxy server 76
5.6 HTTP cache 80

6 Traffic Policy 86
6.1 Network Rules Wizard 86
6.2 How traffic rules work 96
6.3 Definition of Custom Traffic Rules 96
6.4 Basic Traffic Rule Types 106

7 Bandwidth Limiter 113
7.1 How the bandwidth limiter works and how to use it 113
7.2 Bandwidth Limiter configuration 114
7.3 Detection of connections with large data volume transferred 118

8 User Authentication 121
8.1 Firewall User Authentication 121

9 Web Interface 125
9.1 Web Interface Parameters Configuration 125
9.2 Login/logout page 130
9.3 Status information and user statistics 133
9.4 User preferences 134

10 HTTP and FTP filtering 137
10.1 Conditions for HTTP and FTP filtering 138
10.2 URL Rules 138
10.3 Global rules for Web elements 146
10.4 Content Rating System (ISS OrangeWeb Filter) 147
10.5 Web content filtering by word occurrence 151
10.6 FTP Policy 155

11 Antivirus control 160
11.1 Conditions and limitations of antivirus scan 160
11.2 How to choose and setup antiviruses 162
11.3 HTTP and FTP scanning 166
11.4 Email scanning 170

12 Definitions 173
12.1 IP Address Groups 173
12.2 Time Intervals 174
12.3 Services 177
12.4 URL Groups 180

13 User Accounts and Groups 183
13.1 Viewing and definitions of user accounts 184
13.2 Local user accounts 186
13.3 Local user database: external authentication and import of accounts 195
13.4 Active Directory domains mapping 199
13.5 User groups 204

14 Remote Administration and Update Checks 209
14.1 Setting Remote Administration 209
14.2 Update Checking 210

15 Advanced security features 213
15.1 P2P Eliminator 213
15.2 Special Security Settings 216
15.3 VPN using IPSec Protocol 218

16 Other settings 222
16.1 Routing table 222
16.2 Demand Dial 225
16.3 Universal Plug-and-Play (UPnP) 230
16.4 Relay SMTP server 231

17 Status Information 234
17.1 Active hosts and connected users 234
17.2 Show connections related to the selected process 242
17.3 Alerts 246

18 Basic statistics 251
18.1 Interface statistics 251
18.2 User Statistics — data volumes and quotas 254

19 Kerio StaR — statistics and reporting 257
19.1 Monitoring and storage of statistic data 257
19.2 Settings for statistics and quota 258
19.3 Connection to StaR and viewing statistics 261
19.4 Accounting period 263
19.5 Overall View 265
19.6 User statistics 269
19.7 Users by Traffic 270
19.8 Top Visited Websites 271
19.9 Top Requested Web Categories 272

20 Logs 275
20.1 Log settings 275
20.2 Logs Context Menu 278
20.3 Alert Log 283
20.4 Config Log 284
20.5 Connection Log 285
20.6 Debug Log 286

20.7 Dial Log 286
20.8 Error Log 289
20.9 Filter Log 290
20.10 Http log 291
20.11 Security Log 293
20.12 Sslvpn Log 295
20.13 Warning Log 295
20.14 Web Log 296

21 Kerio VPN 298
21.1 VPN Server Configuration 299
21.2 Configuration of VPN clients 304
21.3 Interconnection of two private networks via the Internet (VPN tunnel) 305
21.4 Exchange of routing information 311
21.5 Example of Kerio VPN configuration: company with a filial office 313
21.6 Example of a more complex Kerio VPN configuration 328

22 Kerio Clientless SSL-VPN 355
22.1 Configuration of WinRoute's SSL-VPN 355
22.2 Usage of the SSL-VPN interface 357

23 Troubleshooting 360
23.1 Detection of incorrect configuration of the default gateway 360
23.2 Configuration Backup and Transfer 361
23.3 Automatic user authentication using NTLM 365
23.4 Partial Retirement of Protocol Inspector 369
23.5 User accounts and groups in traffic rules 370
23.6 FTP on WinRoute's proxy server 372

24 Network Load Balancing 375
24.1 Basic Information and System Requirements 375
24.2 Network Configuration 375
24.3 Configuration of the servers in the cluster 377

25 Technical support 380
25.1 Essential Information 380
25.2 Tested in Beta version 381
25.3 Contacts 382

A Legal Presumption 383

B Used open-source libraries 384

Glossary of terms 386

Index 393

Chapter 1

Quick Checklist

In this chapter you can find a brief guide for a quick setup of "*Kerio WinRoute Firewall*" (called briefly "*WinRoute*" in further text). After this setup the firewall should be immediately available and able to share your Internet connection and protect your local network. For a detailed guide refer to the separate *WinRoute — Step-by-Step Configuration* guide.

If you are not sure how to set any of the *Kerio WinRoute Firewall* functions or features, look up the appropriate chapter in this manual. For information about your Internet connection (such as your IP address, default gateway, DNS server, etc.) contact your ISP.

Note: In this guide, the expression *firewall* represents the host where *WinRoute* is (or will be) installed.

1. The firewall must include at least two interfaces — one must be connected to the local network (i.e. the *Ethernet* or *Token Ring* network adapters), another must be connected to the Internet (i.e. analog modem, ISDN adapter, network adapter or PPPoE connection). TCP/IP parameters must be set properly at both/all interfaces.

   Test functionality of the Internet connection and of traffic among hosts within the local network before you run the *WinRoute* installation. This test will reduce possible problems with debugging and error detections.

2. Run *WinRoute* installation. Specify a username and password for access to the administration from the configuration wizard (for details refer to chapters 2.3 and 2.7).

3. Set basic traffic rules using the *Network Rules Wizard* (see chapter 6.1).

4. Run the *DHCP server* and set required IP ranges including their parameters (subnet mask, default gateway, DNS server address/domain name). For details, see chapter 5.4.

5. Check the *DNS Forwarder's* configuration. Define the local DNS domain if you intend to scan the `hosts` file and/or the DHCP server table. For details, see chapter 5.3.

6. Set user mapping from the *Active Directory* domain or create/import local user accounts and groups. Set user access rights. For details see chapter 13.

7. Define IP groups (chapter 12.1), time ranges (chapter 12.2) and URL groups (chapter 12.4), that will be used during rules definition (refer to chapter 12.2).

8. Create URL rules (chapter 10.2) and set the *ISS OrangeWeb Filter* module (chapter 10.4). Set HTTP cache and automatic configuration of browsers (chapter 5.6). Define FTP rules (chapter 10.6).

9. Select an antivirus and define types of objects that will be scanned. If you choose the integrated *McAfee* antivirus application, check automatic update settings and edit them if necessary.

   Note: External antivirus must be installed before it is set, otherwise it is not available in the combo box.

10. Using one of the following methods set TCP/IP parameters for the network adapter of individual LAN clients:

    - *Automatic configuration* — activate the *Obtain an IP address automatically* option. Do not set any other parameters.

    - *Manual configuration* — define IP address, subnet mask, default gateway address, DNS server address and local domain name.

    Use one of the following methods to set the Web browser at each workstation:

    - *Automatic configuration* — activate the *Automatically detect settings* option (*Microsoft Internet Explorer*) or specify URL for automatic configuration (other types of browsers). For details, refer to chapter 5.6.

    - *Manual configuration* — select type of connection via the local network or define IP address and appropriate proxy server port (see chapter 5.5).

Chapter 2

Introduction

2.1 Kerio WinRoute Firewall

Kerio WinRoute Firewall 6.0 is a complex tool for connection of the local network to the Internet and protection of this network from intrusions. It is developed for OS Windows 2000, XP and 2003.

Basic Features

Transparent Internet Access

With Network Address Translation (NAT) technology, the local private network can be connected to the Internet through a single public IP address (static or dynamic). Unlike proxy servers, with NAT technology all Internet services will be accessible from any workstation and it will be possible to run most standard network applications, as if all computers within the LAN had their own connection to the Internet.

Security

The integrated firewall protects all the local network including the workstation it is installed on, regardless of whether the NAT function (IP translation) is used or *WinRoute* is used as a *neutral* router between two networks. *Kerio WinRoute Firewall* offers the same standard of protection found in much more costly hardware solutions.

Relay Control tab

All the security settings within *WinRoute* are managed through so-called traffic policy rules. These provide effective network protection from external attacks as well as easy access to all the services running on servers within the protected local network (e.g. Web Server, Mail server, FTP Server, etc.). Communication rules in the traffic policy can also restrict local users in accessing certain services on the Internet.

Bandwidth Limiter

Typically, problems with Internet connection arise when a user attempts to download big volume of data (installation archive, disk image, audio/video file, etc.) and thus the connection to the Internet and to other server services is slowed down for other users. The *WinRoute's* built-in *Bandwidth Limiter* module enables to reserve bandwidth for transfer of big size data. The rest of the bandwidth will be constantly available for other services.

Protocol Maintenance (Protocol Inspectors)

You may come across applications that do not support the standard communication and that may for instance use incompatible communication protocols, etc. To challenge this problem, *WinRoute* includes so-called protocol inspectors, which identify the appropriate application protocol and modify the firewall's behavior dynamically, such as temporary access to a specific port (it can temporarily open the port demanded by the server). FTP in the active mode, Real Audio or PPTP are just a few examples.

Network Configuration

WinRoute has a built-in DHCP server, which sets TCP/IP parameters for each workstation within your local network. Parameters for all workstations can be set centrally from a single point. This reduces the amount of time needed to set up the network and minimizes the risk of making a mistake during this process.

DNS forwarder module enables easy DNS configuration and faster responses to DNS requests. It is a simple type of caching nameserver that relays requests to another DNS server. Responses are stored in its cache. This significantly speeds up responses to frequent requests. Combined with the DHCP server and the system's `HOSTS` file, the *DNS forwarder* can be also used as a dynamic DNS server for the local domain.

Remote Administration

All settings are performed in the *Kerio Administration Console*, an independent administration console used to manage all Kerio's server products. It can be run either on the workstation with *WinRoute* or on another host within the local network or the Internet. Communication between *WinRoute* and the administration console is encrypted and thus protected from being tapped or misused.

Various Operating Systems Within The Local Network

WinRoute works with standard TCP/IP protocols. From the point of view of workstations within the local network it acts as a standard router and no special client applications are required. Therefore, any operating system with TCP/IP, such as Windows, Unix/Linux, Mac OS etc., can be run within the LAN.

Note: WinRoute can work with TCP/IP protocol sets only. It does not affect the functionality of other protocols (i.e. IPX/SPX, NetBEUI, AppleTalk, etc.).

Additional Features

HTTP and FTP filtering

WinRoute can monitor all HTTP and FTP communication and block objects that do not match given criteria. The settings can be global or defined specifically for each user.

Antivirus control

WinRoute can perform antivirus check of transmitted files. For this purpose, either the built-in *McAfee* antivirus or an external antivirus program (e.g. *NOD32*, *AVG*, etc.) are available. Antivirus check can be applied to *HTTP*, *FTP*, *SMTP* and *POP3* protocols.

Transparent support for Active Directory

If *WinRoute* is employed in a network using the *Active Directory* domain, it is not necessary to create local accounts or import users from the domain as *Active Directory* directory accounts can be used in *WinRoute*. This option simplifies administration of user accounts, especially for greater number of users.

Email alerts

WinRoute can send email alerts informing users about various events. This function makes firewall administration easier for the administrators since they need not connect to *WinRoute* frequently to check it through. All sent alerts are saved in a special log file.

User quotas

A limit can be set for transmitted data per each user. This limit can be set for the amount of downloaded or/and uploaded data per day/month. These limits are called quotas. If any quota is exceeded, the connection to the Internet will be blocked for a corresponding user. Email alert can be optionally sent to the user.

Blocking of P2P networks

WinRoute can detect and block so called Peer-to-Peer networks (networks used for sharing of files, such as *Kazaa*, *DirectConnect* etc.).

StaR — statistics and reporting

Detailed statistics of the firewall interface (current speed of transmitted data, amount of data transmitted in certain time periods) as well as of individual users (amount of transmitted data, used services, categories of connected Websites, etc.) can be viewed in *WinRoute*.

Basic statistics are available in the administration program while detailed statistics can be found in the firewall's web interface.

Kerio VPN — proprietary VPN server and client

WinRoute also provides a proprietary VPN solution which can be applied to the *server-to-server* and *client-to-server* modes. This VPN solution can perform NAT (even multiple) at both ends. The *Kerio VPN Client* client software is included in the *WinRoute* package that can be used for creation of *client-to-server* VPN types (connection of remote clients to local networks).

Clientless SSL-VPN

The role of the VPN solution which requires a special application at the client side can be supplied by remote access to a private network using a web browser. *Clientless SSL-VPN* enables browsing through hosts and shared items in remote networks as well as files downloads and saving. The traffic is secured by *SSL* (*HTTPS*).

2.2 Conflicting software

The *WinRoute* host can be used as a workstation, however it is not recommended as user activity can affect the functionality of the operating system and *WinRoute* in a negative way.

WinRoute can be run with most of common applications. However, there are certain applications that should not be run at the same host as *WinRoute* for this could result in collisions.

Collision of low-level drivers

WinRoute Firewall may collide with applications that use low-level drivers with either identical or similar technology.

- Applications used for Internet connection, such as *Microsoft Proxy Server* and *Microsoft Proxy Client*, etc.
- Network firewalls — i.e. *Microsoft ISA Server*, *CheckPoint Firewall-1*, *WinProxy* (by Ositis), *Sygate Office Network* and *Sygate Home Network*, etc.
- Personal firewalls, such as *Kerio Personal Firewall*, *Zone Alarm*, *Sygate Personal Firewall*, *Norton Personal Firewall*, etc.
- Software designed to create virtual private networks (VPN) — i.e. software applications developed by the following companies: CheckPoint, Cisco Systems, Nortel, etc. There are many such applications and their features vary from vendor to vendor.
  Under proper circumstances, use of the VPN solution included in *WinRoute* is recommended (for details see chapter 21). Otherwise, we recommend you to test a particular VPN server or VPN client with *WinRoute* trial version or to contact our technical support (see chapter 25).
  Note: VPN implementation included in Windows operating system (based on the PPTP protocol) is supported by *WinRoute*.

Port collision

Applications that use the same ports as the firewall cannot be run at the *WinRoute* host (or the configuration of the ports must be modified).
If all services are running, *WinRoute* uses the following ports:

- `53/UDP` — *DNS Forwarder*
- `67/UDP` — *DHCP server*

- `1900/UDP` — *SSDP Discovery* service
- `2869/TCP` — *UPnP Host* service
  The *SSDP Discovery* and *UPnP Host* services are included in the UPnP support (refer to chapter 16.3).
- `44333/TCP+UDP` — traffic between *Kerio Administration Console* and *WinRoute Firewall Engine*. This service cannot be stopped.

The following services use corresponding ports by default. Ports for these services can be changed.

- `443/TCP` — server of the *SSL-VPN* interface (see chapter 22)
- `3128/TCP` — HTTP proxy server (see chapter 5.5)
- `4080/TCP` — Web administration interface (refer to chapter 9)
- `4081/TCP` — secured (SSL-encrypted) version of the Web administration interface (see chapter 9)
- `4090/TCP+UDP` — proprietary VPN server (for details refer to chapter 21)

Antivirus applications

If an antivirus application that scans files on the disk is run on the *WinRoute* host, the HTTP cache file (see chapter 5.6, usually the "/> subdirectory under the directory where *WinRoute* is installed) and the `tmp` subdirectory (used to scan HTTP and FTP objects) must be excluded from inspection. If the antivirus is run manually, there is no need to exclude these files, however, *WinRoute Firewall Engine* must be stopped before running the antivirus (this is not always desirable).

Note: If *WinRoute* uses an antivirus to check objects downloaded via HTTP or FTP protocols (see chapter 11.3), the cache directory can be excluded with no risk — files in this directory have already been checked by the antivirus.

Note: WinRoute can stop automatically The *Windows Firewall / Internet Connection Sharing* system service is not mentioned as problematic, since *WinRoute* can stop automatically. For details, see chapter 2.3.

2.3 Installation

System requirements

Requirements on minimal hardware parameters of the host where *WinRoute* will be installed:

- CPU 1 GHz
- 512 MB RAM
- 2 network interfaces
- 50 MB free disk space (for the installation)
- Disk space for statistics (see chapter 19) and logs (in accordance with traffic flow and logging level — see chapter 20)
- For maximum protection of the installed product (particularly its configuration files), it is recommended to use the *NTFS* file system.

The product supports for the following operating systems:

- Windows 2000 SP4
- Windows XP SP2 (both 32-bit and 64-bit editions)
- Windows Server 2003 SP1 (both 32-bit and 64-bit editions)

Note: The *Client for Microsoft Networks* component must be installed for all supported operating systems, otherwise *WinRoute* will not be available as a service and NTLM authentication will not function. The component is included in installation packages of all supported operating systems.

Steps to be taken before the installation

Install *WinRoute* on a computer which is used as a gateway connecting the local network and the Internet. This computer must include at least one interface connected to the local network (Ethernet, TokenRing, etc.) and at least one interface connected to the Internet. You can use either a network adapter (Ethernet, WiFi, etc.) or a modem (analog, ISDN, etc.) as an Internet interface.

We recommend you to check through the following items before you run *WinRoute* installation:

- Time of the operating system should be set correctly (for timely operating system and antivirus upgrades, etc.)
- The latest service packs and any Microsoft recommended security updates should be applied.
- TCP/IP parameters should be set for all available network adapters
- All network connections (both to the local network and to the Internet) should function properly. You can use for example the `ping` command to detect time that is needed for connections.

These checks and pre-installation tests may protect you from later problems and complications.

Note: Basic installation of all supported operating systems include all components required for smooth functionality of *WinRoute*.

Installation and Basic Configuration Guide

Once the installation program is launched (i.e. through `kerio-kwf-6.3.0-1100-win.exe`), a guide will take you through setting the basic firewall parameters.

You will be asked to choose among three types of installation — *Typical*, *Compact* (minimal, i.e with no help issues) or *Custom*. Choosing the custom mode will let you select *WinRoute's* individual components:

- *Kerio WinRoute Firewall Engine* — core of the application
- *VPN Support* — proprietary VPN solution developed by Kerio Technologies,
- *Administration Console* — the *Kerio Administration Console* application (universal console for all server applications of *Kerio Technologies*),
- *Help Files* — this manual in the *HTML Help* format. For help files details, see *Kerio Administration Console — Help* (`http://www.kerio.com/kwf-manual`).

Go to chapter 2.4 for a detailed description of all *WinRoute* components. For detailed description on the proprietary VPN solution, refer to chapter 21.

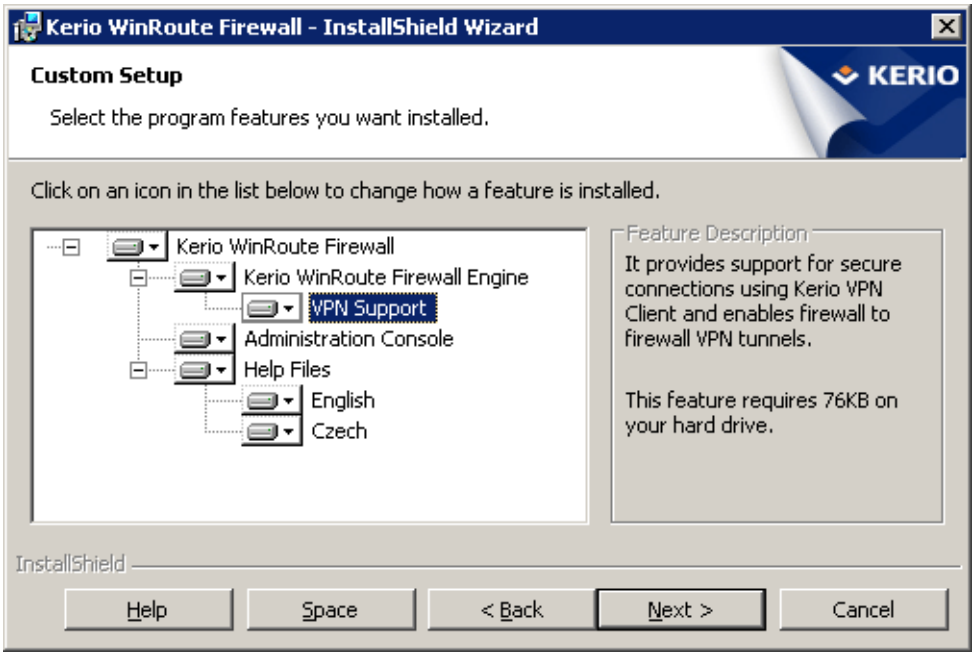

Kerio WinRoute Firewall - InstallShield Wizard
Custom Setup
Select the program features you want installed.
KERIO
Click on an icon in the list below to change how a feature is installed.
Kerio WinRoute Firewall
Kerio WinRoute Firewall Engine
VPN Support
Administration Console
Help Files
English
Czech
Feature Description
It provides support for secure connections using Kerio VPN Client and enables firewall to firewall VPN tunnels.
This feature requires 76KB on your hard drive.
InstallShield
Help
Space
< Back
Next >
Cancel

Figure 2.1 Custom installation — selecting optional components

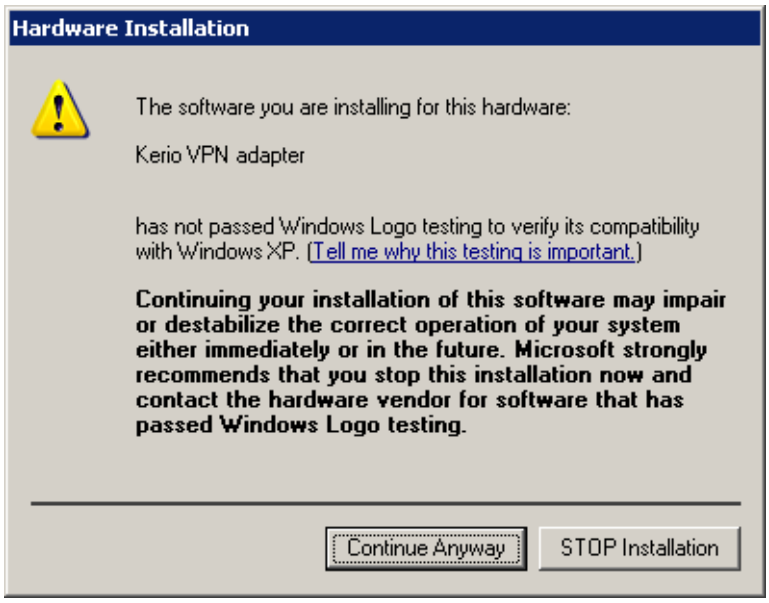

Hardware Installation
The software you are installing for this hardware:
Kerio VPN adapter
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

Figure 2.2 Installation — verifying compatibility of the low-level driver with Windows XP

Notes:

1. During the installation process of the *WinRoute's* low-level drivers, the operating system may display a warning message informing that compatibility of the drivers with the Windows operating system cannot be verified (this depends on configuration of

the operating system).

However, the drivers provided within the *WinRoute* installation package have been tested on all supported Windows operating systems. Therefore, these drivers may be considered as compatible.

The *Kerio WinRoute Firewall Device* low-level driver (*Kerio WinRoute Firewall Driver — Lower Layer*) is required to be installed for each network adapter. Therefore, the total number of alerts depends on the number of network adapters in the system.

2. If you selected the *Custom* installation mode, the behavior of the installation program will be as follows:

   - all checked components will be installed or updated
   - all checked components will not be installed or will be removed

   During an update, all components that are intended to remain must be ticked.

Having completed this step, you can start the installation process. All files will be copied to the hard disk and all the necessary system settings will be performed. The initial Wizard will be run automatically after your first login (see chapter 2.7).

Under usual circumstances, a reboot of the computer is not required after the installation (a restart may be required if the installation program rewrites shared files which are currently in use). This will install the *WinRoute* low-level driver into the system kernel. *WinRoute Engine* will be automatically launched when the installation is complete. The engine runs as a service.

Protection of the installed product

To provide the firewall with the highest security possible, it is necessary to ensure that undesirable (unauthorized) persons has no access to the critical files of the application, especially to configuration files. If the *NTFS* system is used, *WinRoute* refreshes settings related to access rights to the directory (including all subdirectories) where the firewall is installed upon each startup. Only members of the *Administrators* group and local system account (*SYSTEM*) are assigned the full access (read/write rights), other users are not allowed access the directory.

Warning: If the *FAT32* file system is applied, it is not possible to secure *WinRoute* files in the way described above. For this reason, it is recommended to install *WinRoute* only on computers which use the *NTFS* file system.

Conflicting Applications and System Services

The *WinRoute* installation program detects applications and system services that might conflict with the *WinRoute Firewall Engine*.

1. *Windows Firewall's* system components[1] and *Internet Connection Sharing*.

   These components provide the same low-level functions as *WinRoute*. If they are running concurrently with *WinRoute*, the network communication would not be functioning correctly and *WinRoute* might be unstable. Both components are run by the *Windows Firewall / Internet Connection Sharing* system service.[2].

   Warning: To provide proper functionality of *WinRoute*, it is *necessary* that the *Internet Connection Firewall / Internet Connection Sharing detection* is stopped and forbidden!

2. *Universal Plug and Play Device Host* and *SSDP Discovery Service*

   The services support *UPnP* (Universal Plug and Play) in the Windows XP and Server 2003 operating systems. However, these services collide with the *UPnP* support in *WinRoute* (refer to chapter 16.3).

The *WinRoute* installation includes a dialog where it is possible to disable colliding system services.

By default, the *WinRoute* installation disables all the colliding services listed. Under usual circumstances, it is not necessary to change these settings. Generally, the following rules are applied:

- The *Windows Firewall / Internet Connection Sharing (ICS)* service should be disabled. Otherwise, *WinRoute* will not work correctly. The option is a certain kind of warning which informs users that the service is running and that it should be disabled.
- To enable support for the *UPnP* protocol in *WinRoute* (see chapter 16.3), it is necessary to disable also services *Universal Plug and Play Device Host* and *SSDP Discovery Service*.
- If you do not plan to use support for *UPnP* in *WinRoute*, it is not necessary to disable the *Universal Plug and Play Device Host* and *SSDP Discovery Service*services.

Notes:

1. Upon each startup, *WinRoute* detects automatically whether the *Windows Firewall / Internet Connection Sharing* is running. If it is, *WinRoute* stops it and makes a record

[1] In *Windows XP Service Pack 1* and older versions, the integrated firewall is called *Internet Connection Firewall*

[2] In the older *Windows* versions listed above, the service is called *Internet Connection Firewall / Internet Connection Sharing*.

Kerio WinRoute Firewall - InstallShield Wizard
System Service Conflict
Conflict with the system services has been detected.
KERIO
Kerio WinRoute Firewall is conflicting with several system services. It is highly recommended to disable them.
Windows Firewall/Internet Connection Sharing (ICS)
Disable this system service
Universal Plug and Play Device Host
Disable this system service
SSDP Discovery Service
Disable this system service
Installation setup will change the configuration of the selected services to disable them from start. If you are unsure, disable the system service.
InstallShield
< Back
Next >
Cancel

Figure 2.3 Disabling colliding system services during installation

in the *warning* log. This helps assure that the service will be enabled immediately after the *WinRoute* installation.

2. In *Windows XP Service Pack 2*, *WinRoute* automatically registers in the *Security Center*. This implies that the *Security Center* always indicates firewall status correctly and it does not display warnings informing that the system is not protected.

2.4 WinRoute Components

Kerio WinRoute consists of the three following components:

WinRoute Firewall Engine
: is the core of the program that provides all services and functions. It is running as a service in the operating system (the service is called *Kerio WinRoute Firewall* and it is run automatically within the system account by default).

WinRoute Engine Monitor
: Allows viewing and modification of the *Engine's* status (stopped/running) and setting of start-up preferences (i.e. whether *Engine* and/or *Monitor* should be run automatically at system start-up). It also provides easy access to the *Administration Console*. For details, refer to chapter 2.5.

Note: WinRoute Firewall Engine is independent on the *WinRoute Engine Monitor*. The *Engine* can be running even if there is no icon in the System Tray on Windows or in the Dock in Mac OS X.

Kerio Administration Console

It is a versatile console for local or remote administration of Kerio server products. For successful connection to an application you need a plug-in with an appropriate interface. *Kerio Administration Console* is installed hand-in-hand with the appropriate module during the installation of *Kerio WinRoute*. Detailed guidance for *Kerio Administration Console* is provided in *Kerio Administration Console — Help* (`http://www.kerio.com/kwf-manual`).

2.5 WinRoute Engine Monitor

WinRoute Engine Monitor is a standalone utility used to control and monitor the *WinRoute Firewall Engine* status. The icon of this component is displayed on the toolbar.

Figure 2.4 WinRoute Engine Monitor icon in the Notification Area

If *WinRoute Engine* is stopped, a white crossed red spot appears on the icon. Under different circumstances, it can take up to a few seconds to start or stop the *WinRoute Engine* application. Meanwhile, the icon gets grey and is inactive — does not respond to mouse clicking.

On Windows, left double-clicking on this icon runs the *Kerio Administration Console* (described later). Use the right mouse button to open the following menu:

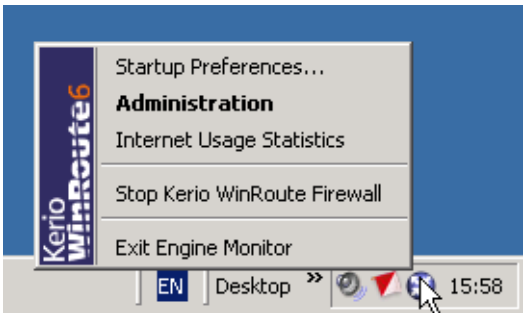


Figure 2.5 WinRoute Engine Monitor menu

Start-up Preferences
With these options *WinRoute Engine* and/or *WinRoute Engine Monitor* applications can be set to be launched automatically when the operating system is started. Both options are enabled by default.

Administration
Runs *Kerio Administration Console* (equal to double-clicking on the *WinRoute Engine Monitor* icon).

Internet Usage Statistics
Opens *Internet Usage Statistics* in the default browser. For details, see chapter 19.

Start / Stop WinRoute Firewall
Switches between the Start and Stop modes. The text displays the current mode status.

Exit Engine Monitor
An option to exit *WinRoute Engine Monitor*. It does not affect status of the *WinRoute Engine* application (this will be announced by a report).

Notes:

1. If a limited version of *WinRoute* is used (e.g. a trial version), a notification is displayed 7 days before its expiration. This information is displayed until the expiration.

2. *WinRoute Engine Monitor* is available in English only.

2.6 Upgrade and Uninstallation

In this chapter you can find a description of *WinRoute* upgrade within the versions `5.x` and `6.x` (i.e. upgrade from the `5.1.10` version to the `6.3.0` version or from `6.3.0` to `6.3.1`). Direct upgrade from `4.x` versions or earlier to the `6.x` version is not supported.

Simply run the installation of a new version to upgrade *WinRoute* (i.e. to get a new release from the *Kerio* Web pages — `http://www.kerio.com/`).

All windows of the *Kerio Administration Console* must be closed before the (un)installation is started. All of the three *WinRoute* components will be stopped and closed automatically.

The installation program detects the directory with the former version and updates it by replacing appropriate files with the new ones automatically. License, all logs and user defined settings are kept safely.

Uninstallation

To uninstall *WinRoute*, stop all three *WinRoute* components. The *Add/Remove Programs* option in the *Control Panel* launches the uninstallation process. All files under the *WinRoute* directory can be optionally deleted.

(typically the path `C:\Program Files\Kerio\WinRoute Firewall`)

— configuration files, SSL certificates, license key, logs, etc.

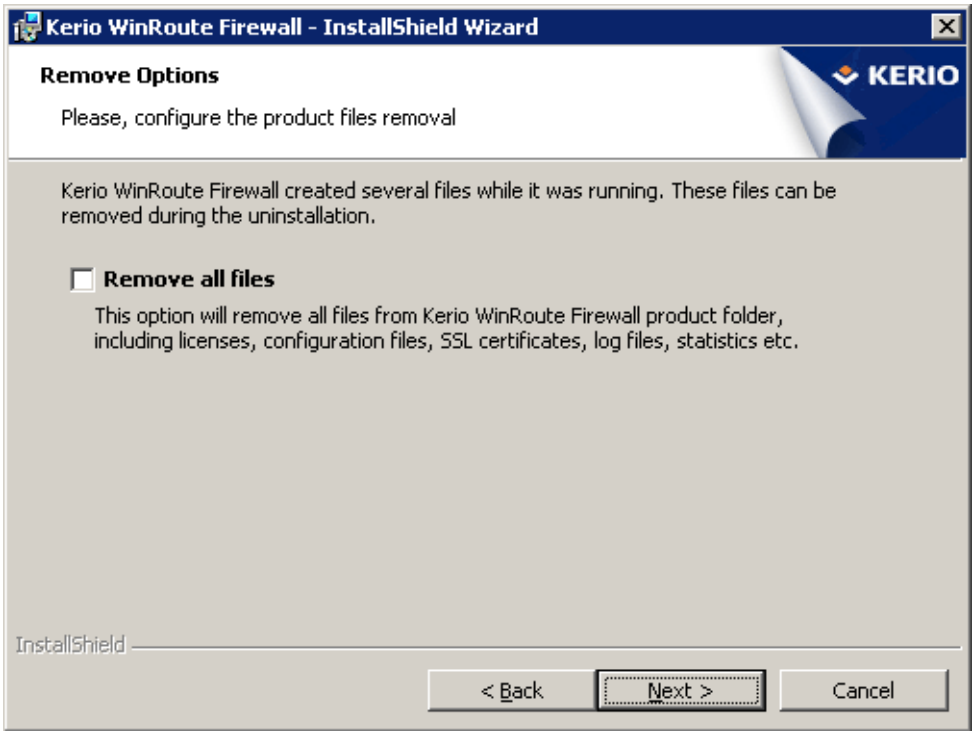

Kerio WinRoute Firewall - InstallShield Wizard
Remove Options
Please, configure the product files removal
KERIO
Kerio WinRoute Firewall created several files while it was running. These files can be removed during the uninstallation.
Remove all files
This option will remove all files from Kerio WinRoute Firewall product folder, including licenses, configuration files, SSL certificates, log files, statistics etc.
InstallShield
< Back
Next >
Cancel

Figure 2.6 Uninstallation — asking user whether files created in WinRoute should be deleted

Keeping these files may be helpful for copying of the configuration to another host or if it is not sure whether the SSL certificates were issued by a trustworthy certification authority.

During uninstallation, the *WinRoute* installation program automatically refreshes the original status of the *Windows Firewall / Internet Connection Sharing*, *Universal Plug and Play Device Host*) and *SSDP Discovery Service* system services.

Upgrade from WinRoute Pro 4.x

To import your configuration used in *WinRoute Pro 4.x* to the *Kerio WinRoute Firewall 6.x*, follow these steps:

1. Upgrade the *WinRoute Pro 4.x* to the *Kerio WinRoute Firewall 5.x*. Version 5.x includes a tool for initial configuration, which is able to read and translate the configuration from the *WinRoute Pro 4.x*.

2. Upgrade version 5.x to version 6.x (see above).

Note: This method of upgrade is not recommended. Do not use it unless necessary (e.g. a great amount of user accounts to be imported). Configuration parameters of the *WinRoute Pro 4.x* have crucial differences and only some of the parameters can be imported. Later revisions and error removals might be more exigent than a brand new configuration.

Update Checker

WinRoute enables automatic checks for new versions of the product at the *Kerio Technologies* website. Whenever a new version is detected, its download and installation will be offered automatically.

For details, refer to chapter 14.2.

2.7 Configuration Wizard

Using this Wizard you can define all basic *WinRoute* parameters. It is started automatically by the installation program.

Note: In any language version, the configuration wizard is available in English only.

Setting of administration username and password

Definition of the administration password is essential for the security of the firewall. Do not use the standard (blank) password, otherwise unauthorized users may be able to access the *WinRoute* configuration.

Password and its confirmation must be entered in the dialog for account settings. The administrator's username (`Admin` is used as default) can be edited in the *Username* text field.

Note: If the installation is running as an upgrade, this step is skipped since the administrator account already exists.

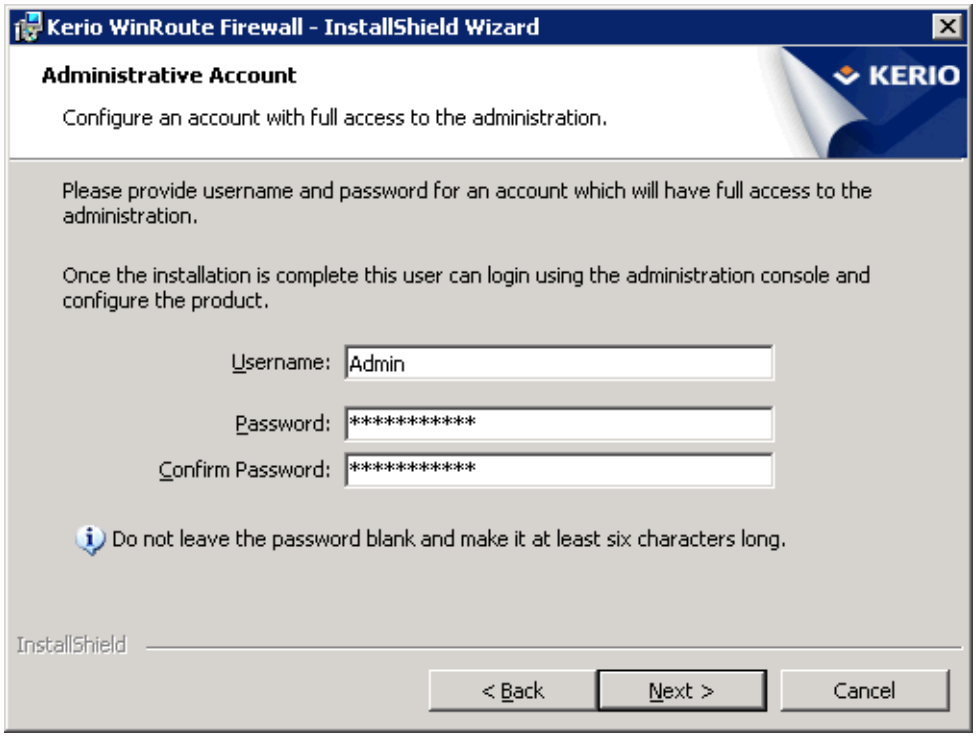

Kerio WinRoute Firewall - InstallShield Wizard
Administrative Account
Configure an account with full access to the administration.
KERIO
Please provide username and password for an account which will have full access to the administration.
Once the installation is complete this user can login using the administration console and configure the product.
Username:
Admin
Password:
Confirm Password:
Do not leave the password blank and make it at least six characters long.
InstallShield
< Back
Next >
Cancel

Figure 2.7 Initial configuration — Setting of administration username and password

Remote Access

Immediately after the first *WinRoute Firewall Engine* startup all network traffic will be blocked (desirable traffic must be permitted by traffic rules — see chapter 6). If *WinRoute* is installed remotely (i.e. using terminal access), communication with the remote client will be also interrupted immediately (*WinRoute* must be configured locally).

Within Step 2 of the configuration wizard specify the IP address of the host from which the firewall will be controlled remotely (i.e. using terminal services) to enable remote installation and administration. Thus *WinRoute* will enable all traffic between the firewall and the remote host.

Note: Skip this step if you install *WinRoute* locally. Allowing full access from a point might endanger security.

Enable remote access

This option enables full access to the *WinRoute* computer from a selected IP address

Remote IP address

IP address of the computer from where you will be connecting (e.g. terminal services client). This field must contain an IP address. A domain name is not allowed.

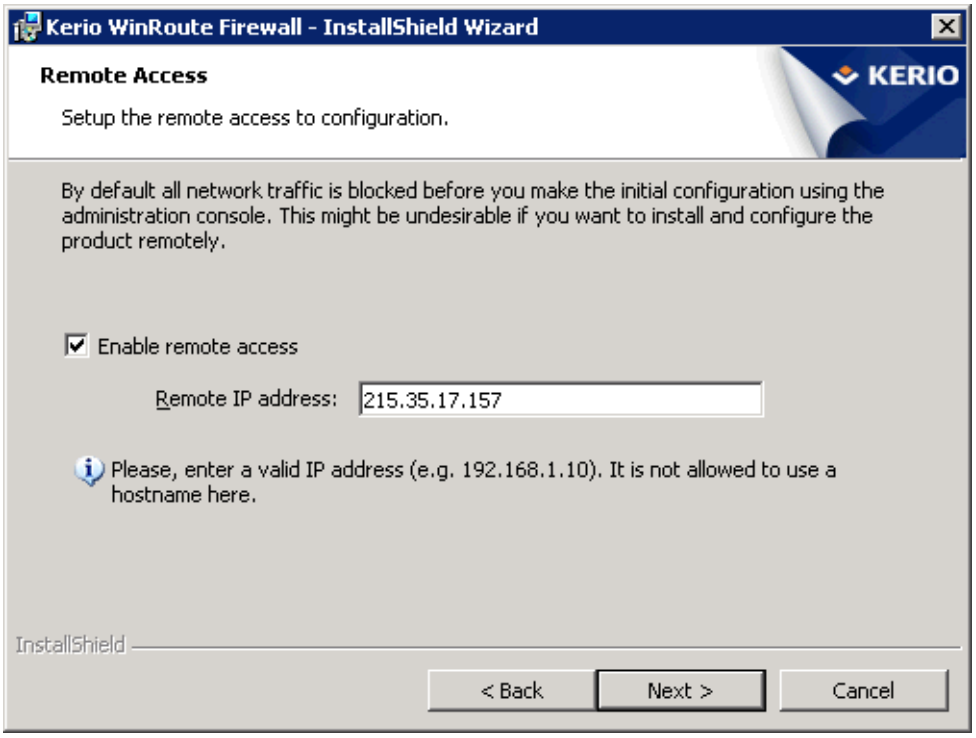

Kerio WinRoute Firewall - InstallShield Wizard
Remote Access
Setup the remote access to configuration.
KERIO
By default all network traffic is blocked before you make the initial configuration using the administration console. This might be undesirable if you want to install and configure the product remotely.
Enable remote access
Remote IP address:
215.35.17.157
Please, enter a valid IP address (e.g. 192.168.1.10). It is not allowed to use a hostname here.
InstallShield
< Back
Next >
Cancel

Figure 2.8 Initial configuration — Allowing remote administration

Warning: The remote access rule is disabled automatically when *WinRoute* is configured using the network policy wizard (see chapter 6.1).

Chapter 3

WinRoute Administration

All Kerio products including *WinRoute* are administered through the *Kerio Administration Console* application(an application used for administration of all Kerio Technologies' server products; thereinafter *Administration Console*). Using this program you can access *WinRoute Firewall Engine* either locally (from the *Engine* host) or remotely (from another host). Traffic between *Administration Console* and *WinRoute Firewall Engine* is encrypted. This protects you from tapping and misuse.

The *Administration Console* is installed along with *WinRoute* (see chapters 2.3 and 2.4). For its usage details, see *Administration Console — Help* (`http://www.kerio.com/kwf-manual`).

The following chapters of this guide provide descriptions on individual sections of the *WinRoute* administration dialog window which is opened upon a successful login to the *WinRoute Firewall Engine*.

Notes:

1. *Administration Console* for *WinRoute* is available in English, Spanish, Czech and Slovak.

2. Upon the first login to *WinRoute* after a successful installation, the traffic rules wizard is run so that the initial *WinRoute* configuration can be performed. For a detailed description on this wizard please refer to chapter 6.16.1.

3.1 Administration Window

The main *WinRoute* administration dialog window ("administration window") will be opened upon a successful login to the *WinRoute Firewall Engine* through the *Administration Console*. This window is divided into two parts:

- The left column contains the tree view of sections. The individual sections of the tree can be expanded and collapsed for easier navigation. *Administration Console* remembers the current tree settings and uses them upon the next login.

- In the right part of the window, the contents of the section selected in the left column is displayed (or a list of sections in the selected group).

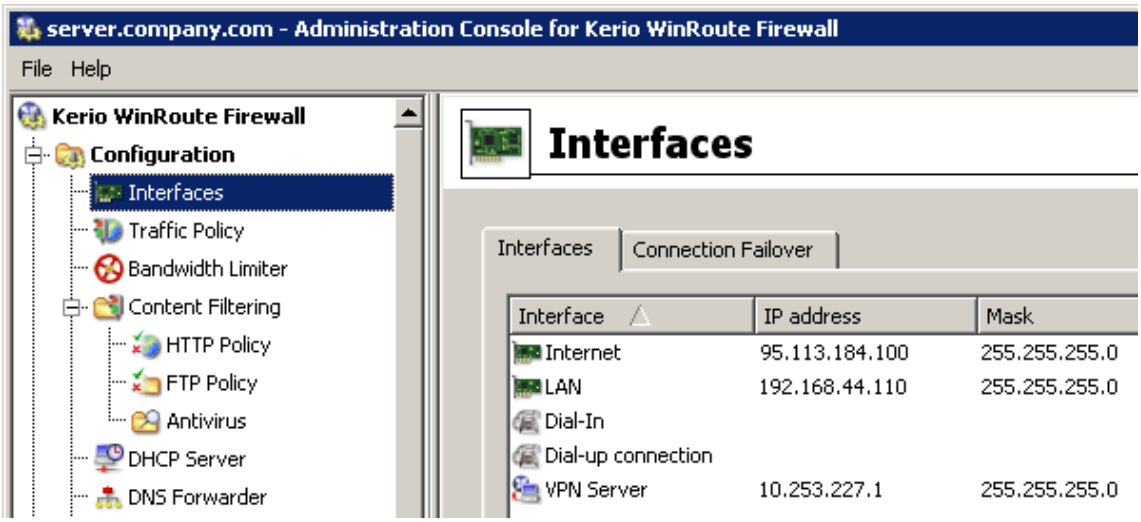


Figure 3.1 The main window of Administration Console for WinRoute

Administration Window — Main menu

The main menu provides the following options:

File

- *Reconnect* — reconnection to the *WinRoute Firewall Engine* after a connection drop-out (caused for example by a restart of the *Engine* or by a network error).
- *New connection* — opens the main window of the *Administration Console*. Use a bookmark or the login dialog to connect to a server.
  This option can be useful when the console will be used for administration of multiple server applications (e.g. *WinRoute* at multiple servers). For details, see *Administration Console — Help* (`http://www.kerio.com/kwf-manual`).
  Note: The *New Connection* option opens the same dialog as running the *Administration Console* from the *Start* menu.
- *Quit* — this option terminates the session (users are logged out of the server and the administration window is closed). The same effect can be obtained by clicking the little cross in the upper right corner of the window or pressing *Alt+F4*.

Help menu

- *Administrator's guide* — this option displays the administrator's guide in *HTML Help* format. For help details, see *Administration Console — Help* (`http://www.kerio.com/kwf-manual`).
- *About* — this page provides information about current version of the application (*WinRoute's* administration module in this case), a link to our company's website, etc.

Status bar

The status bar at the bottom of the administration window displays the following information (from left to right):

Figure 3.2 Administration Console status bar

- The section of the administration window currently selected in the left column. This information facilitates navigation in the administration window when any part of the section tree is not visible (e.g. when a lower screen resolution is selected).
- Name or IP address of the server and port of the server application (*WinRoute* uses port 44333).
- Name of the user logged in as administrator.
- Current state of the *Administration Console*: *Ready* (waiting for user's response), *Loading* (retrieving data from the server) or *Saving* (saving changes to the server).

Detection of WinRoute Firewall Engine connection drop-out

Administration Console is able to detect the connection failure automatically. The failure is usually detected upon an attempt to read/write the data from/to the server (i.e. when the *Apply* button is pressed or when a user switches to a different section of *Administration Console*). In such case, a connection failure dialog box appears where the connection can be restored.

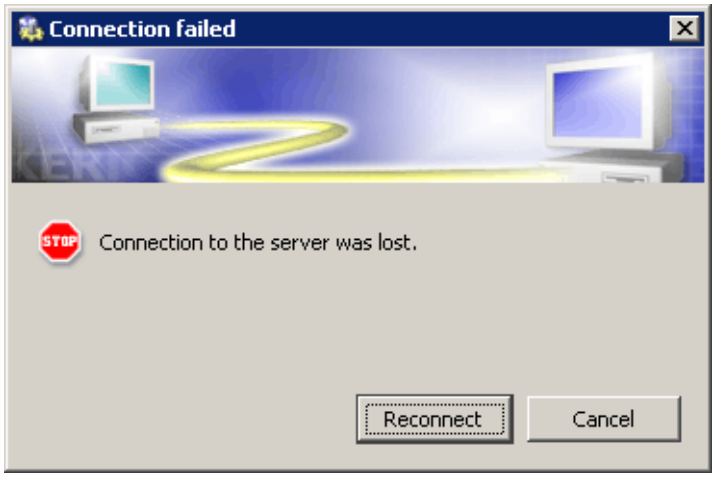


Figure 3.3 Detection of WinRoute Firewall Engine connection drop-out

After you remove the cause of the connection failure, the connection can be restored. If the reconnection attempt fails, only the error message is shown. You can then try to reconnect using the *File* → *Restore connection* option from the main menu, or close the window and restore the connection using the standard procedure.

3.2 View Settings

Many sections of the *Administration Console* are in table form where each line represents one record (e.g. detailed information about user, information about interface, etc.) and the columns consist of individual entries for these records (e.g. name of server, MAC address, IP address, etc.).

WinRoute administrators can define — according to their liking — the way how the information in individual sections will be displayed. When you right-click each of the above sections, a pop-up menu with *Modify columns* option is displayed. This entry opens a dialog window where users can select which columns will be displayed/hidden.

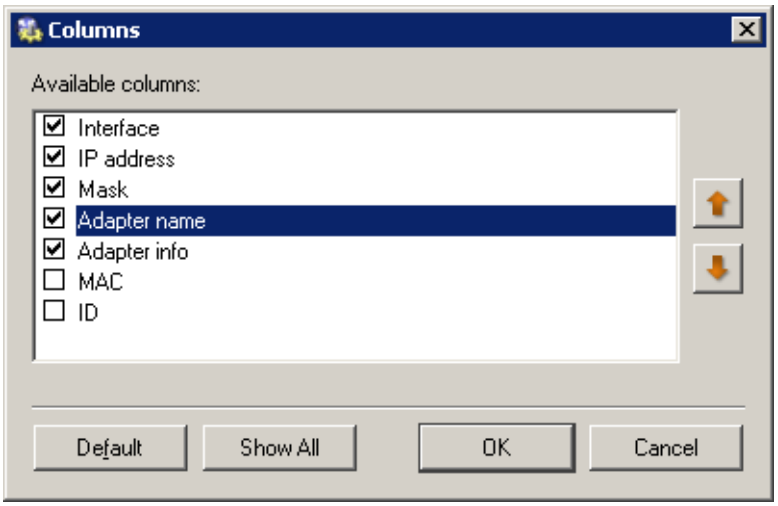


Figure 3.4 Column customization in Interfaces

This dialog offers a list of all columns available for a corresponding view. Use checking boxes on the left to enable/disable displaying of a corresponding column. You can also click the *Show all* button to display all columns. Clicking on the *Default* button will restore default settings (for better reference, only columns providing the most important information are displayed by default).

The arrow buttons move the selected column up and down within the list. This allows the administrator to define the order the columns will be displayed.

The order of the columns can also be adjusted in the window view. Left-click on the column name, hold down the mouse button and move the column to the desired location.

Note: The width of individual columns can be adjusted by moving the dividing line between the column headers.

Chapter 4

Product Registration and Licensing

When purchased, *Kerio WinRoute Firewall* must be registered. *WinRoute* must be registered at Kerio Technologies website (`http://www.kerio.com/`) after the purchase. So called license key will be generated upon a successful registration(the `license.key` file) that to be imported to *WinRoute* (refer to chapter 4.2). If the key is not imported, *WinRoute* will behave as a full-featured trial version and its license will be limited by the expiration timeout.

This also implies that the only difference between a trial version and full *WinRoute* version is whether the registration key has been imported or not. This gives each customer an opportunity to test and try the product in the particular environment during the 30-day period. Then, once the product is purchased, the customer can simply register the installed version by the purchased license number (see chapter 4.3). This means that it is not necessary to uninstall the trial version and reinstall the product.

Once the 30-day trial period expires, *WinRoute* cuts the speed of all network traffic of the computer where it is installed to 4 KB/s. Also, the routing is blocked (which means that the computer cannot be used as a gateway for the Internet).

Full functionality in *WinRoute* will be available after a valid license key is imported.

Note: If the license key is lost (e.g. is removed, etc.), it is possible to register the product again at the *Kerio Technologies* website and download the key (only the purchase number of the basic product is required during a repeated registration).

4.1 License types and number of users

License types (optional components)

WinRoute can optionally include the following components: *McAfee* antivirus (refer to chapter 11) or/and the *ISS OrangeWeb Filter* module for web pages rating (see chapter 10.4). These components are licensed individually.

License keys consist of the following information:

WinRoute license
: Basic *WinRoute* license. Its validity is defined by the two following factors:

- update right expiration date — specifies the date by which *WinRoute* can be updated for free. When this date expires, *WinRoute* keeps functioning, however, it cannot be updated. The time for updates can be extended by purchasing a subscription.
- product expiration date — specifies the date by which *WinRoute* stops functioning and blocks all TCP/IP traffic at the host where it is installed. If this happens, a new valid license key must be imported or *WinRoute* must be uninstalled.

McAfee license

This license is defined by the two following dates:

- update right expiration date (independent of *WinRoute*) — when this date expires, the antivirus keeps functioning, however, neither its virus database nor the antivirus can be updated yet.
  Warning: Owing to persistent incidence of new virus infections we recommend you to use always the most recent antivirus versions.
- plug-in expiration date— specifies the date by which the antivirus stops functioning and cannot be used anymore.

ISS OrangeWeb Filter license

ISS OrangeWeb Filter module is provided as a service. License is defined only by an expiration date which specifies when this module will be blocked.

Note: Refer to Kerio Technologies Website (`http://www.kerio.com/`) to get up-to-date information about individual licenses, subscription extensions, etc.

Deciding on a number of users (licenses)

WinRoute's license key includes information about maximal number of users allowed to use the product. In accordance with the licensing policy, number of users is number of hosts protected by *WinRoute*, i.e. sum of the following items:

- All hosts in the local network (workstations and servers),
- all possible VPN clients connecting from the Internet to the local network.

The host where *WinRoute* is installed in not included in the total number of users.

Warning: If the maximal number of licensed users is exceeded, *WinRoute* may block traffic of some hosts!

4.2 License information

The license information can be displayed by selecting *Kerio WinRoute Firewall* (the first item in the tree in the left part of the *Administration Console* dialog window — this section is displayed automatically whenever the *WinRoute* administration is entered).

Figure 4.1 Administration Console welcome page providing license information

Product
: name of the product (*WinRoute*)

Copyright
: Copyright information.

Homepage
: Link to the *Kerio WinRoute Firewall* homepage (information on pricing, new versions, etc.). Click on the link to open the homepage in your default browser.

Operational system
: Name of the operating system on which the *WinRoute Firewall Engine* service is running.

License ID
License number or a special license name.

Subscription expiration date
Date until when the product can be upgraded for free.

Product expiration date
Date when the product expires and stops functioning (only for trial versions or special license types).

Number of users
Maximal number of hosts (unique IP addresses) that can be connected to the Internet via *WinRoute* at the same time (for details, refer to chapter 4.6).

Company
Name of the company (or a person) to which the product is registered.

Depending on the current license, links are displayed at the bottom of the image:

1. For unregistered versions:

   - *Become a registered trial user* — registration of the trial version. This type of registration is tentative and it is not obligatory. The registration provides users free technical support for the entire trial period.

   - *Register product with a purchased license number* — registration of a purchased product.

     Once purchased, the product must be registered. Otherwise, it will keep behaving as a trial version!

2. For registered versions:

   - *Update registration info* — this link can be used to update information about the person/company to which the product is registered and/or to add subscription license numbers or add-on licenses (add users).

For details on registration of *WinRoute* from *Administration Console*, refer to chapter 4.4.

If the update checker is enabled (refer to chapter 14.2), the *A new version is available, click here for details...* notice is displayed whenever a new version is available. Click on the link to open the dialog where the new version can be downloaded and the installation can be started (for details, see chapter 14.2).

Note: Click the right mouse button at the *Administration Console* welcome page to open the menu providing the following options:

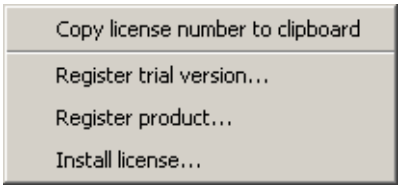


Figure 4.2 The Administration Console's welcome page pop-up menu

- *Copy license number to clipboard* — copies the license number (the *ID licence* item) to the clipboard. This may be helpful e.g. when ordering an upgrade or subscription, where the number of the base license is required, or when sending an issue to the *Kerio Technologies* technical support.
- *Register trial version* — registration of the product's trial version.
- *Register product* — registration of a product with a purchased license number.
- *Install license* — import of the license key (received against the registration at the website — see chapter 4.4).

4.3 Registration of the product in the Administration Console

Since version *6.2.0*, it is possible to register *WinRoute* from the *Administration Console* by following a corresponding link in the welcome page (see chapter 4.2).

Registration of the trial version

By registrating the trial version, users get free email and telephonic technical support for the entire trial period. In return, *Kerio Technologies* gets valuable feedback from these users. Registration of the trial version is not obligatory. However, it is recommended since it provides certain benefits. Such a registration *does not oblige* users to purchase the product.

Clicking on *Become a registered trial user* launches the registration wizard.

1. On the first page of the wizard, read the security code displayed in the picture and type it to the text field (this protects the registration server from misuse). The security code is not case-sensitive.

2. On the second page, enter information about the trial version user (person, company). It is also necessary that the user accepts the *Privacy Policy Terms*. Otherwise, the information cannot be stored in the *Kerio Technologies* database.

   Use the *E-mail address* textfield to enter a valid email address. It is recommended to use the address of the user who is performing the registration. At this address, confirmation of the registration will be demanded when the registration is completed.

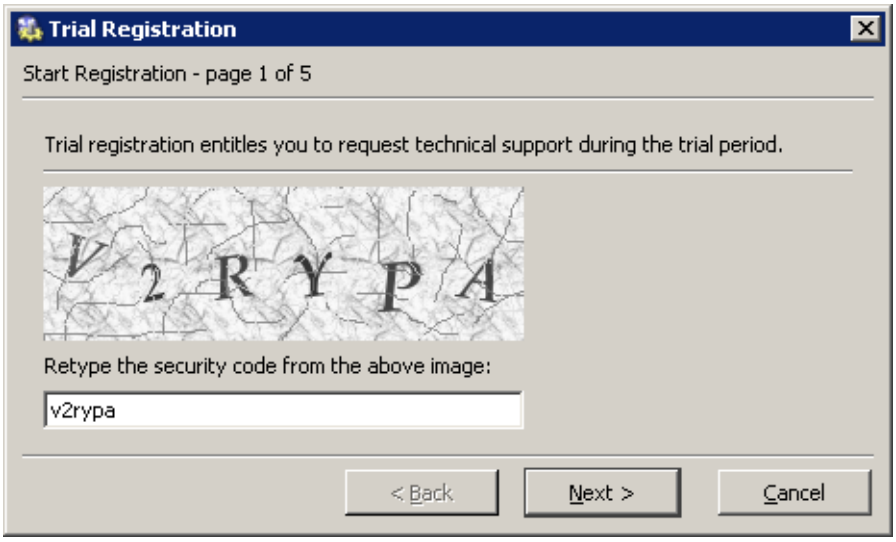

Trial Registration
Start Registration - page 1 of 5
Trial registration entitles you to request technical support during the trial period.
Retype the security code from the above image:
v2rypa
< Back
Next >
Cancel

Figure 4.3 Trial version registration — security code

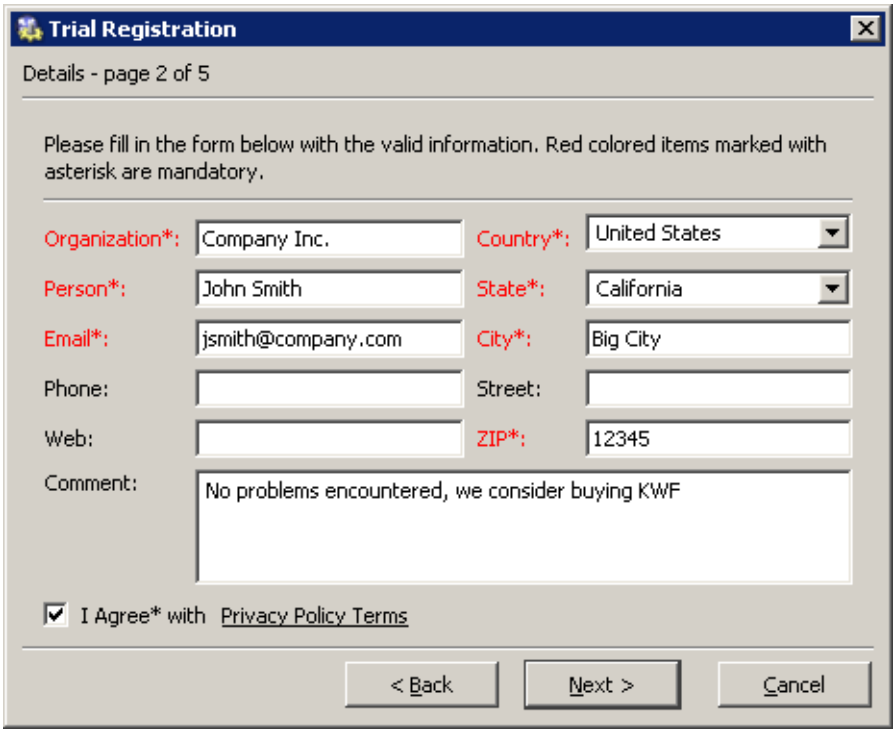


Figure 4.4 Trial version registration — user information

3. Page three includes optional information. Is is not obligatory to answer these questions, however, the answers help *Kerio Technologies* accommodate demands of as many customers as possible.

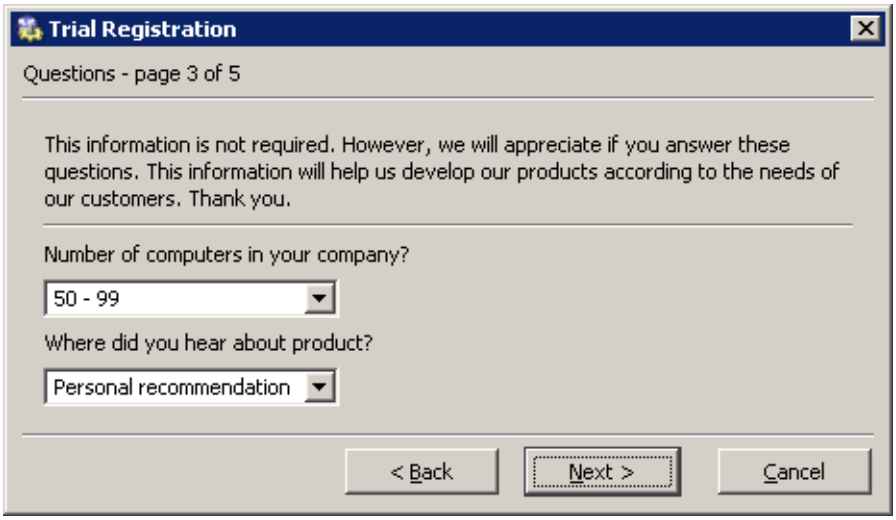

Trial Registration
Questions - page 3 of 5
This information is not required. However, we will appreciate if you answer these questions. This information will help us develop our products according to the needs of our customers. Thank you.
Number of computers in your company?
50 - 99
Where did you hear about product?
Personal recommendation
< Back
Next >
Cancel

Figure 4.5 Trial version registration — other information

4. The fourth page provides the information summary. If any information is incorrect, use the *Back* button to browse to a corresponding page and correct the data.

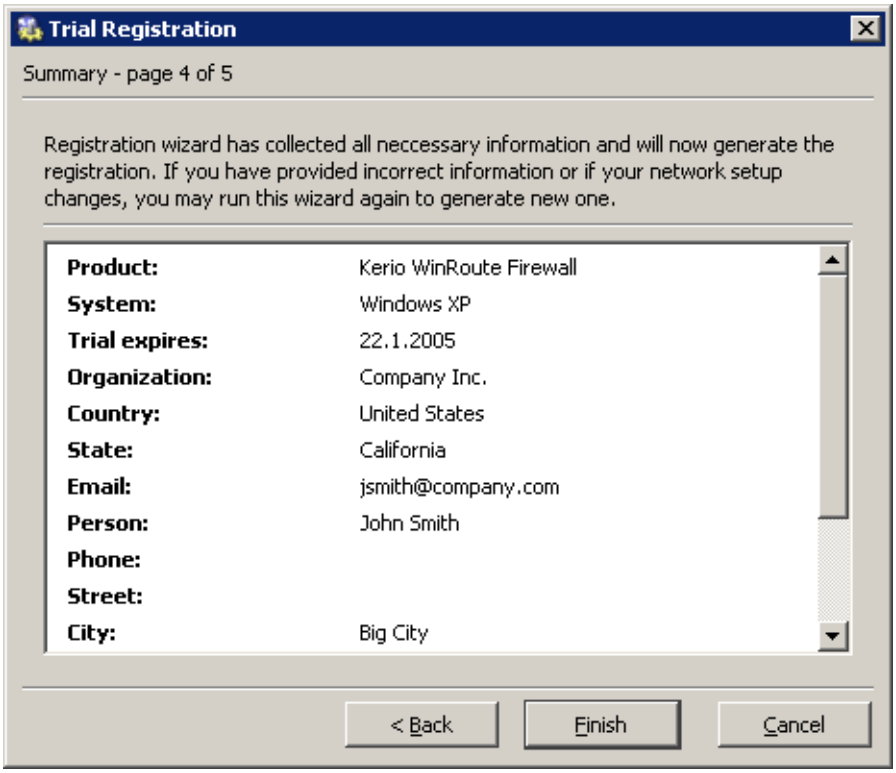

Trial Registration
Summary - page 4 of 5
Registration wizard has collected all neccessary information and will now generate the registration. If you have provided incorrect information or if your network setup changes, you may run this wizard again to generate new one.
Product: Kerio WinRoute Firewall
System: Windows XP
Trial expires: 22.1.2005
Organization: Company Inc.
Country: United States
State: California
Email: jsmith@company.com
Person: John Smith
Phone:
Street:
City: Big City
< Back
Finish
Cancel

Figure 4.6 Registration of the trial version — summary

5. The last page of the wizard provides user's *Trial ID*. This is ID is a unique code used for identification of the registered user when asking help at our technical support.

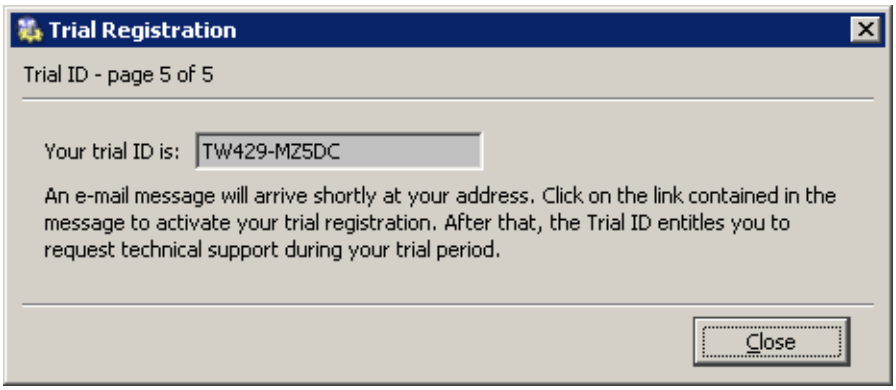

Trial Registration
Trial ID - page 5 of 5
Your trial ID is:
TW429-MZ5DC
An e-mail message will arrive shortly at your address. Click on the link contained in the message to activate your trial registration. After that, the Trial ID entitles you to request technical support during your trial period.
Close

Figure 4.7 Trial version registration — Trial ID

At this point, an email message (in the language set in the *Administration Console*) where confirmation of the registration is demanded is sent to the email address specified on the page two of the wizard. Click on the link in the email message to complete the registration and to make the *Trial ID* valid. The main purpose of the confirmation process is to check that the email address is valid and that the user really wants to be registered.

Registration of the purchased product

Follow the *Register product with a purchased license number* link to run the registration wizard.

1. On the first page of the wizard, it is necessary to enter the license number of the basic product delivered upon its purchase and retype the security code displayed at the picture in the text field (this protects the server from misuse). The security code and the license number are not case-sensitive.

2. On the second page, it is possible to specify license numbers of add-ons (added users), optional components and subscriptions. The page also includes any license numbers associated with the basic product that have already been registered.

   Click on *Add* to add purchased license numbers. Each number is checked immediately. Only valid license numbers are accepted.

   The license numbers added recently can be edited or removed. Registered license numbers (recorded in previous registrations) cannot be removed.

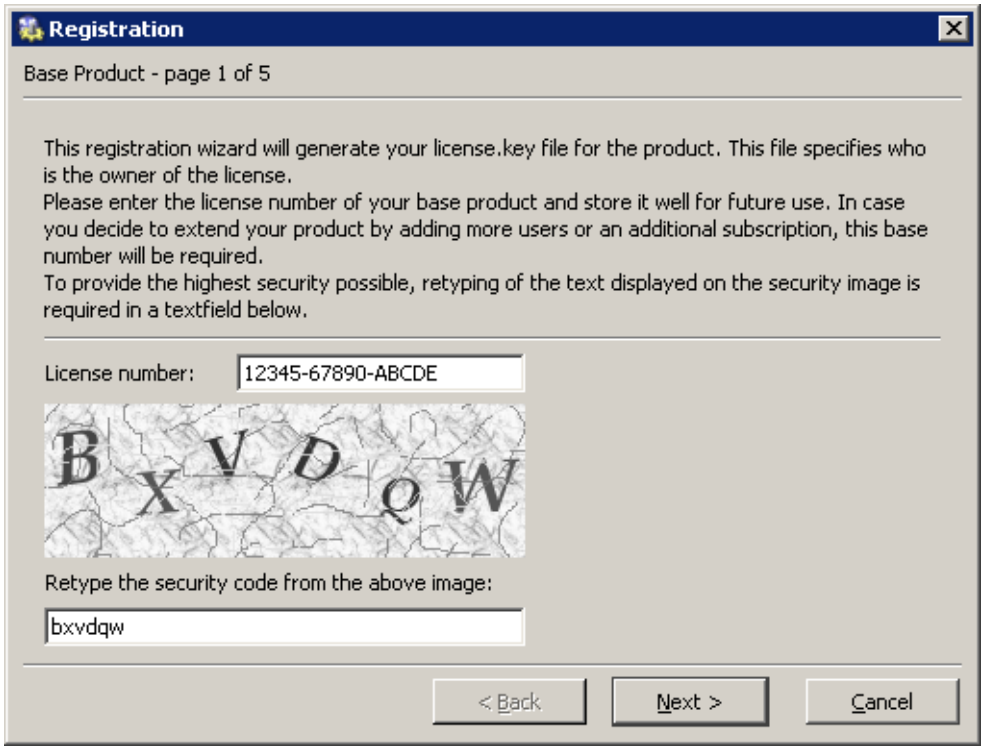

Registration
Base Product - page 1 of 5
This registration wizard will generate your license.key file for the product. This file specifies who is the owner of the license.
Please enter the license number of your base product and store it well for future use. In case you decide to extend your product by adding more users or an additional subscription, this base number will be required.
To provide the highest security possible, retyping of the text displayed on the security image is required in a textfield below.
License number:
12345-67890-ABCDE
Retype the security code from the above image:
bxvdqw
< Back
Next >
Cancel

Figure 4.8 Product registration — license number of the basic product and the security code

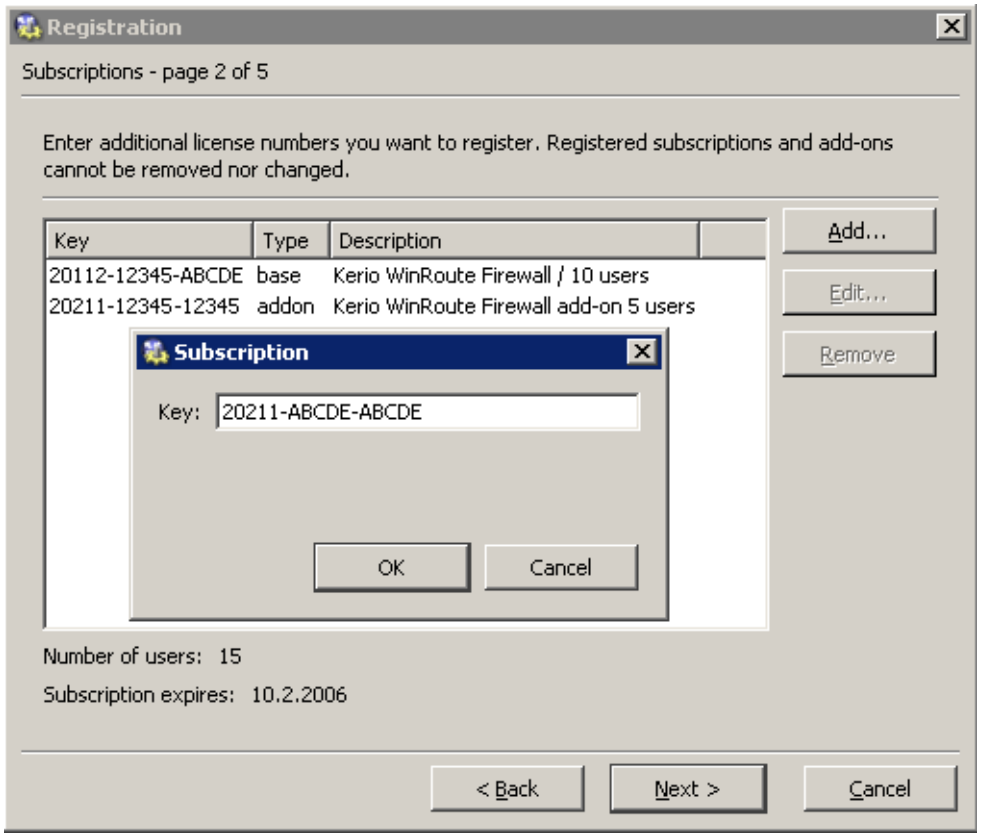


Figure 4.9 Product registration — license numbers of additional components, add-ons and subscription

3. On the third page, enter information about the user (person, company). It is also necessary that the user accepts the *Privacy Policy Terms*. Otherwise, the information cannot be stored in the *Kerio Technologies* database.

   Use the *E-mail address* textfield to enter a valid email address. It is recommended to use the address of the user who is performing the registration. At this address, confirmation of the registration will be demanded when the registration is completed.

4. Page four includes optional information. Is is not obligatory to answer these questions, however, the answers help *Kerio Technologies* accommodate demands of as many customers as possible.

   These questions are asked only during the primary (original) registration. If these questions have already been answered, the page is skipped and the registration process consists of four steps only.

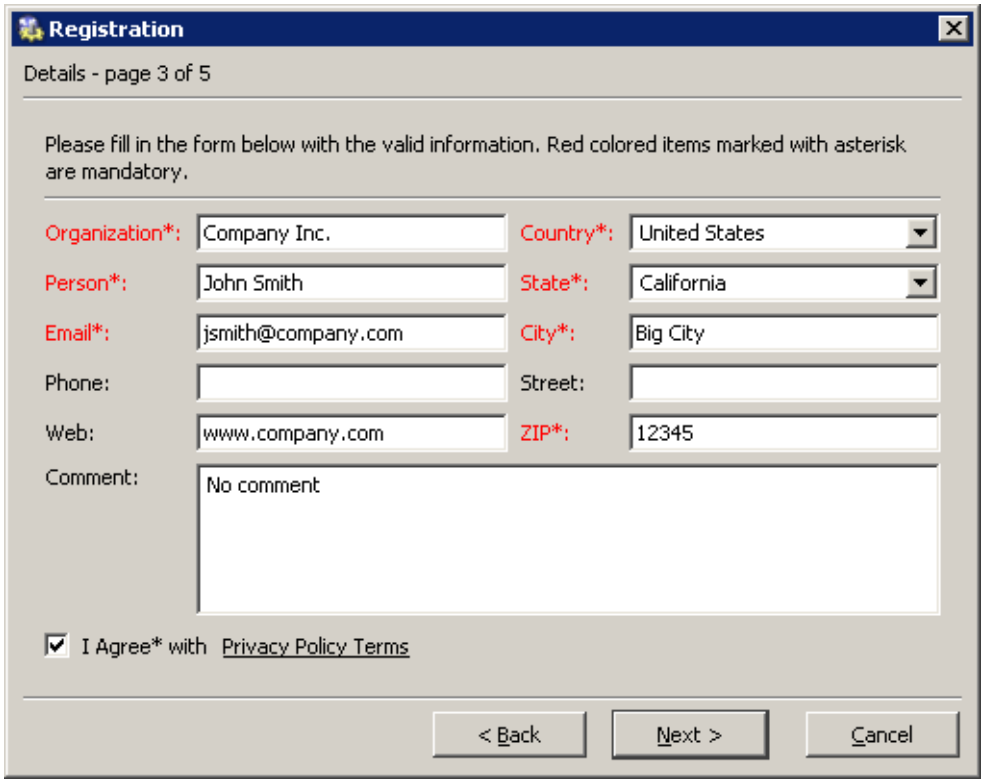


Figure 4.10 Product registration — user information

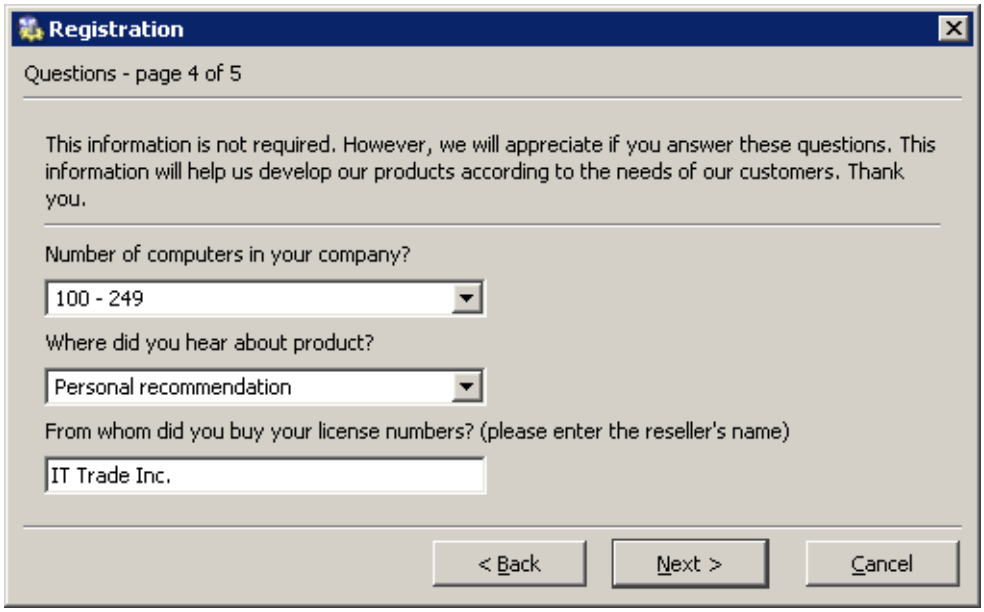

Registration
Questions - page 4 of 5
This information is not required. However, we will appreciate if you answer these questions. This information will help us develop our products according to the needs of our customers. Thank you.
Number of computers in your company?
100 - 249
Where did you hear about product?
Personal recommendation
From whom did you buy your license numbers? (please enter the reseller's name)
IT Trade Inc.
< Back
Next >
Cancel

Figure 4.11 Product registration — other information

5. The last page provides the information summary. If any information is incorrect, use the *Back* button to browse to a corresponding page and correct the data.

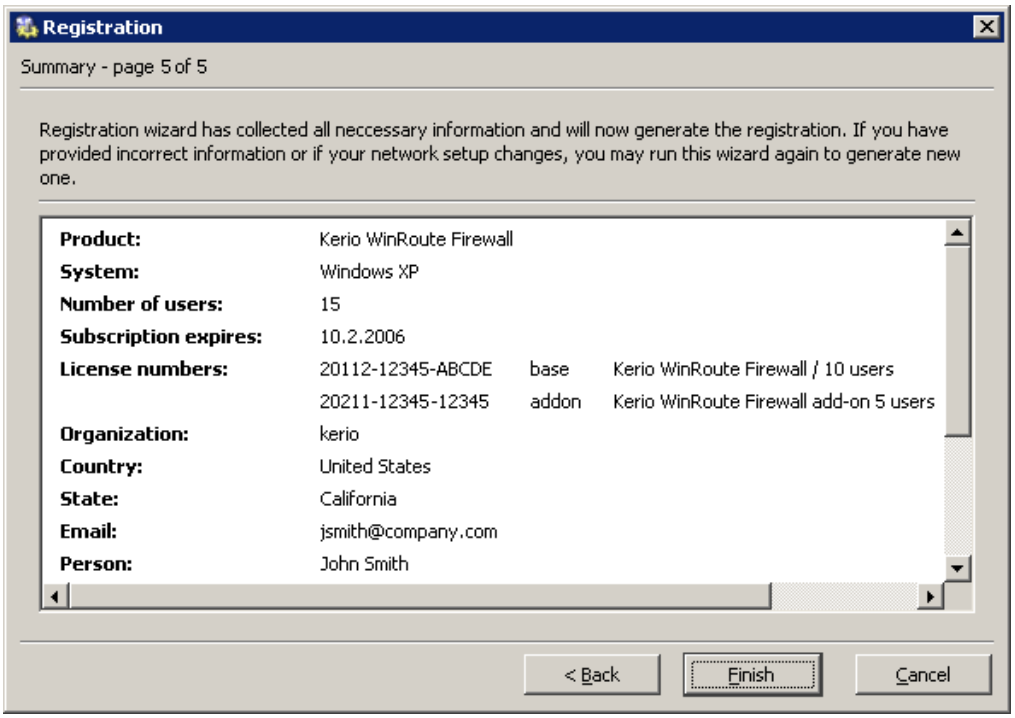

Registration
Summary - page 5 of 5
Registration wizard has collected all neccessary information and will now generate the registration. If you have provided incorrect information or if your network setup changes, you may run this wizard again to generate new one.
Product: Kerio WinRoute Firewall
System: Windows XP
Number of users: 15
Subscription expires: 10.2.2006
License numbers: 20112-12345-ABCDE base Kerio WinRoute Firewall / 10 users
20211-12345-12345 addon Kerio WinRoute Firewall add-on 5 users
Organization: kerio
Country: United States
State: California
Email: jsmith@company.com
Person: John Smith
< Back
Finish
Cancel

Figure 4.12 Product registration — summary

Click on *Finish* to use the information to generate a unique license key. The new license is applied immediately (restart is not required).

Note: If an error is reported upon finishing of the registration process (e.g. failure of network connection, etc.), simply restart the wizard and repeat the registration.

Update of registration information

If *WinRoute* is already registered, the *Update registration info* link is displayed at the *Administration Console's* welcome page. Click on the link to run the registration wizard (as described above) with the information preset as defined within the previous registration process. The same method as the for the primary registration can be used to add license numbers and/or to update user information.

4.4 Product registration at the website

If, by any reason, registration of *WinRoute* cannot be performed from the *Administration Console*, it is still possible to register the product at *Kerio Technologies* website. The registration form can be found under *Purchase* → *License Registration*. The form is almost identical with the registration process described in chapter 4.3.

The corresponding license key file is based on the registration form and it is automatically generated upon its completion and confirmation.

Two methods can be used to install the license key:

- Click on *Install License* in the welcome page's pop-up context menu (see figure 4.2). Click this link to open the standard system dialog for opening of a file.

  If the installation of the license key is completed successfully, the license is activated immediately. Information about the new license is displayed on the *Administration Console* welcome page.

  This method can also be used for remote installation of the license key (the license key file must be saved on the disk of the host from which the remote installation is performed).

- By copying the license key file to a corresponding directory.

  The license key must be saved in the `license` folder in the *WinRoute's* installation directory.

  (the typical path is `C:\Program Files\Kerio\WinRoute Firewall\license`).

  It is necessary that the file name (`license.key`) is not changed!

  To activate the license, it is necessary to restart (stop and run again) the *WinRoute Firewall Engine*.

Note: If possible, it is recommended to register *WinRoute* from the *Administration Console* (it is not necessary to restart the *WinRoute Firewall Engine*).

4.5 Subscription / Update Expiration

WinRoute automatically alerts the administrator in case the *WinRoute* license's expiration date, the expiration of the *McAfee* antivirus or of *ISS OrangeWeb Filter* and/or expiration of the update rights (so called subscription) for *WinRoute* or the *McAfee* antivirus is coming soon. These alert only inform the administrator that they should prolong the subscription of *WinRoute* or renew the corresponding license.

Administrators are informed in two ways:

- By a pop-up bubble tip (this function is featured by the *WinRoute Engine Monitor* module),
- by an pop-up window upon a login to the *Administration Console* (only in case of expiration of subscription).

Note: WinRoute administrators can also set posting of license or subscription expiration alerts by email or SMS (see chapter 17.3).

Bubble alerts

Seven days before the date, the *WinRoute Engine Monitor* utility starts to display the information about number of days remaining to the subscription/license expiration several times a day (in regular intervals).

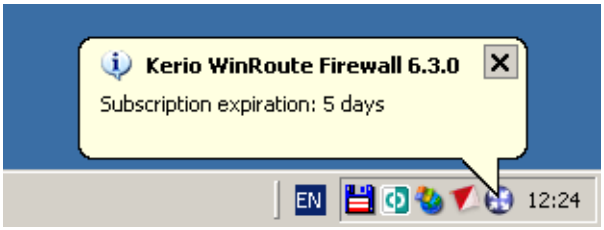


Figure 4.13 License or subscription expiration notice

This information is displayed until *WinRoute* or any of its components stops functioning or *WinRoute* or *McAfee* subscription expires. The information is also stopped being displayed immediately after the registration of the subscription or a license of a particular component (for details, see chapter 4.3).

Notices in the Administration Console

Starting 30 days ago a subscription expiration, a warning informing about number of the days left to the expiration or informing that the subscription has already expired is displayed upon each login. The warning also contains a link to the *Kerio Technologies* website where you can find detailed subscription information as well as order subscription for an upcoming period.

The warning stops being displayed when a license number of a new subscription is registered (refer to chapter 4.3).

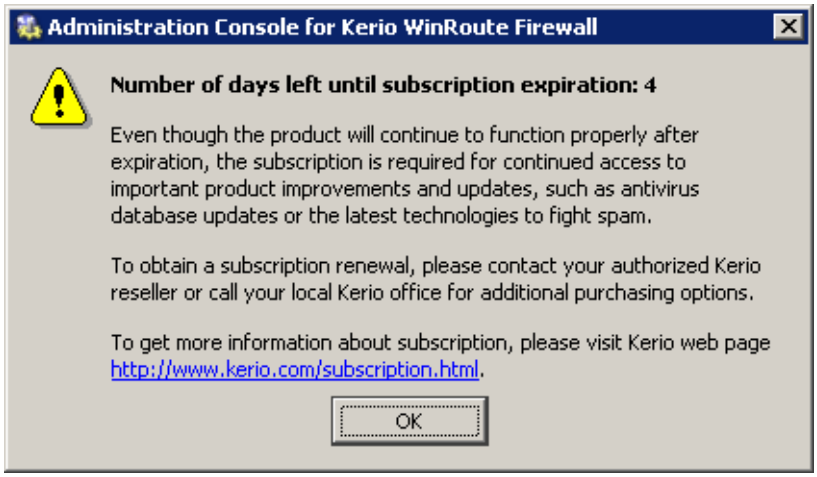

Administration Console for Kerio WinRoute Firewall
Number of days left until subscription expiration: 4
Even though the product will continue to function properly after expiration, the subscription is required for continued access to important product improvements and updates, such as antivirus database updates or the latest technologies to fight spam.
To obtain a subscription renewal, please contact your authorized Kerio reseller or call your local Kerio office for additional purchasing options.
To get more information about subscription, please visit Kerio web page http://www.kerio.com/subscription.html.
OK

Figure 4.14 The notice informing about upcoming subscription expiration

Administration Console for Kerio WinRoute Firewall
The subscription for this product has expired.
Even though the product will continue to function properly after expiration, the subscription is required for continued access to important product improvements and updates, such as antivirus database updates or the latest technologies to fight spam.
To obtain a subscription renewal, please contact your authorized Kerio reseller or call your local Kerio office for additional purchasing options.
To get more information about subscription, please visit Kerio web page http://www.kerio.com/subscription.html.
OK

Figure 4.15 The notice that the subscription has already expired

4.6 User counter

This chapter provides a detailed description on how *WinRoute* checks whether number of licensed users has not been exceeded.

The *WinRoute* license does not limit number of user accounts. Number of user accounts does not affect number of licensed users.

Warning: The following description is only a technical hint that may be used for troubleshooting. License policy must be borne in mind when deciding for a license purchase — see chapter 4.1!

The license counter works as follows:

Start WinRoute

Upon *WinRoute* is started, the table of clients include the firewall only. Number of used licenses is zero.

Note: Table of clients is displayed in the *Active Hosts* section in the *Administration Console* — see chapter 17.1.

License counter

Whenever a communication of any *WinRoute's* client is detected, the IP address is used to identify whether a record does already exist in the table of clients. If not, a new record including the IP address is added to the table and the number of licenses is raised by 1.

The following items are considered as clients:

1. All hosts from which users are connected to the firewall
2. All clients of the *WinRoute's* proxy server (see chapter 5.5)
3. All local hosts communication of which is routed between Internet interfaces and *WinRoute's* local interfaces. The following items belong to this group:
   - Each host which is connected to the Internet while no user is authenticated from the host,
   - All local servers mapped from the Internet,
   - All VPN clients connected to the local network from the Internet.

Licenses are not limited by:

- DNS requests handled by *DNS Forwarder* (*Warning*: If clients use a DNS server located outside the local network, such communication is considered as communication with the Internet),
- DHCP traffic (using either the *WinRoute's DHCP server* or another DHCP server installed on the *WinRoute* host),
- Local communication between the firewall (e.g. access to shared disks) and hosts from which no user is connected to the firewall.

License release

Idleness time (i.e. time for which no packet with a corresponding IP address meeting all conditions is detected) is monitored for each record in the table of clients. If the idleness time of a client reaches 15 minutes, the corresponding record is removed from the table and the number of licenses is decreased by 1. Released license can be used by another host.

Chapter 5

Settings for Interfaces and Network Services

5.1 Network interfaces

WinRoute functions as a router for all *WinRoute's* network interfaces installed within the system. The interfaces are listed in the *Configuration* → *Interface* section of the administration console.

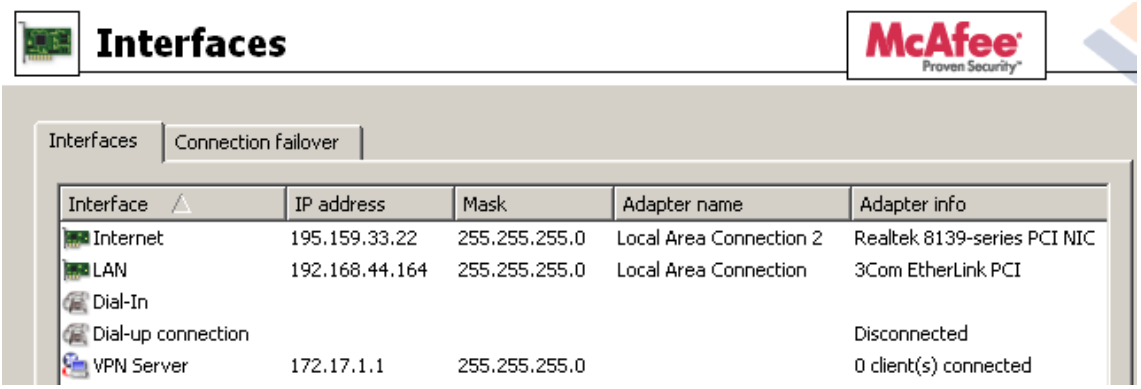


Figure 5.1 Network interfaces

Interface

The name used for interface identification within *WinRoute*. It should be unique for easy reference, e.g. *Internet* for the interface connected to the Internet connection. We recommend you not to use duplicate interface names as they could cause problems during traffic policy definitions or routing table modifications.

The name can be edited later (see below) with no affect on *WinRoute's* functionality.

The icon to the left of the name represents the interface type (network adapter, dial-up connection, VPN server, VPN tunnel).

Note: Unless the name is edited manually, this item displays the name of the adapter as assigned by the operating system (see the *Adapter name* entry).

IP Address and Mask

IP address and the mask of this interface's subnet.

Adapter name

The name of the adapter (e.g. "LAN connection 2"). The name is for reference only.

Adapter info
Adapter identification string returned by the device driver.

ID
A unique identifier of the adapter in the operating system (see also chapter 23.2).

MAC
Hardware (MAC) address of a corresponding network adapter.

Use the buttons at the bottom of the interface list to remove or edit properties of the chosen interface. If no interface is chosen or the selected interface does not support a certain function, appropriate buttons will be inactive.

Add
Adds a new dial-up interface or a VPN channel (see below).
New adapters added must be installed and configured in the operating system. Then, *WinRoute* detects it automatically.

Modify
Displays detailed information and enables editing of the interface's parameters.

Remove
Removes the selected interface from *WinRoute*. This can be done under the following conditions:

- the dial-up is hung-up
- the network adapter is not active or it is not physically present

WinRoute does not allow removing an active network or dial-up adapter.
Notes:

1. Records on adapters that do not exist any longer (those that have been removed) do not affect *WinRoute's* functionality — such adapters are considered as inactive (as in case of a hung-up dial-up).
2. When an adapter is removed, the *Nothing* value is automatically used for corresponding items of all traffic rules where the interface was used. These rules will be disabled. This ensures that the traffic policy is not endangered (for details, refer to chapter 6.3).

Dial or Hang Up /Enebale, Disable
Function of these buttons depend on the interface selected:

- For dial-ups, the *Dial* and *Hang-up* buttons are available and they are used to handle the line by hand.
  Note: You can use *WinRoute's* Web interface (see chapter 9) to dial or hang up lines.
- For VPN tunnels, the *Enable* and *Disable* buttons are available that can be used to enable /disable the VPN tunnel selected for details, see chapter 21.3).

- If a network adapter, a *Dial-in* interface or a VPN server is selected, these buttons are inactive.

Refresh
Use this button to refresh the list of interfaces.

Note: Up to 128 IP addresses can be used for each network interface.

Special interfaces

In addition to network adapters, the following two interfaces are provided in the *Interfaces* section:

Dial-In
This interface represents the server of the *RAS* service (dial-up connection to the network) on the *WinRoute* host. This interface can be used for definition of traffic rules (see chapter 6) for RAS clients which are connecting to this server.
The *Dial-In* interface cannot be configured or removed.
Notes:

1. If both RAS server and *WinRoute* are used, the RAS server must be configured to assign clients IP addresses of a subnet which is not used by any segment of the local network. *WinRoute* performs standard IP routing which might not function unless f this condition is met.
2. For assigning of IP addresses to RAS clients connecting directly to the *WinRoute* host, *it is not possible* to use the *WinRoute's* DHCP server. For details, see chapter 5.4.

VPN server
This interface represents a server which provides a connection for the proprietary VPN client of Kerio Technologies. Double-click on this interface or click on *Edit* to edit settings and parameters of the VPN server. The *VPN server* interface cannot be removed.
For detailed information on the proprietary VPN solution integrated in *WinRoute*, refer to chapter 21.

Adding Interfaces

Click on the *Add* button to add a new interface, either a dial-up or a VPN tunnel (i.e. *server-to-server* VPN connection).

The following text describes only new dial-up connections. Description on how to add a VPN tunnel is provided in chapter 21.3.

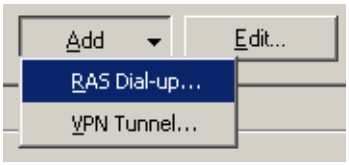


Figure 5.2 Interface type selection

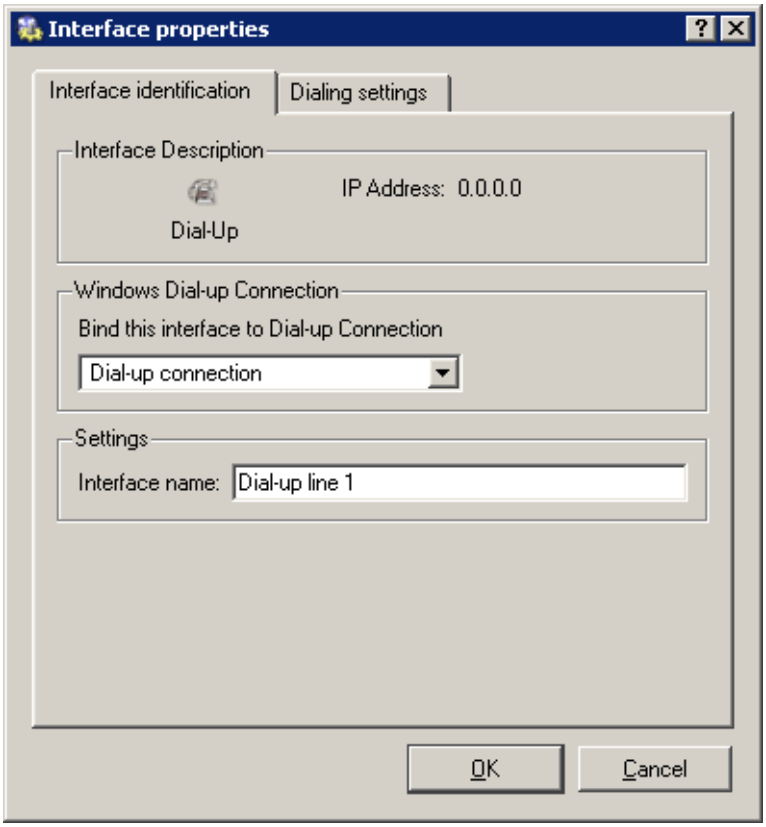


Figure 5.3 Dial-ups — basic parameters

Bind this interface...

Select the Windows RAS connection that you use to connect to your ISP.
Notes:

1. *WinRoute* searches for connections only in the system "phonebook". When creating a new connection for *WinRoute* it is necessary to set that dial-up connections are available to all users, otherwise the operating system saves a corresponding dial-up connection in the profile of the user who created it and *WinRoute* will not be able to find the connection).
2. We recommend you to test any dial-up connection you create before *WinRoute* is installed.

Interface name
Unique name that will identify the line within *WinRoute*.

In the *Dialing Settings* tab you can specify the details of when and how the line will be dialed. Manual dialing is set as default.

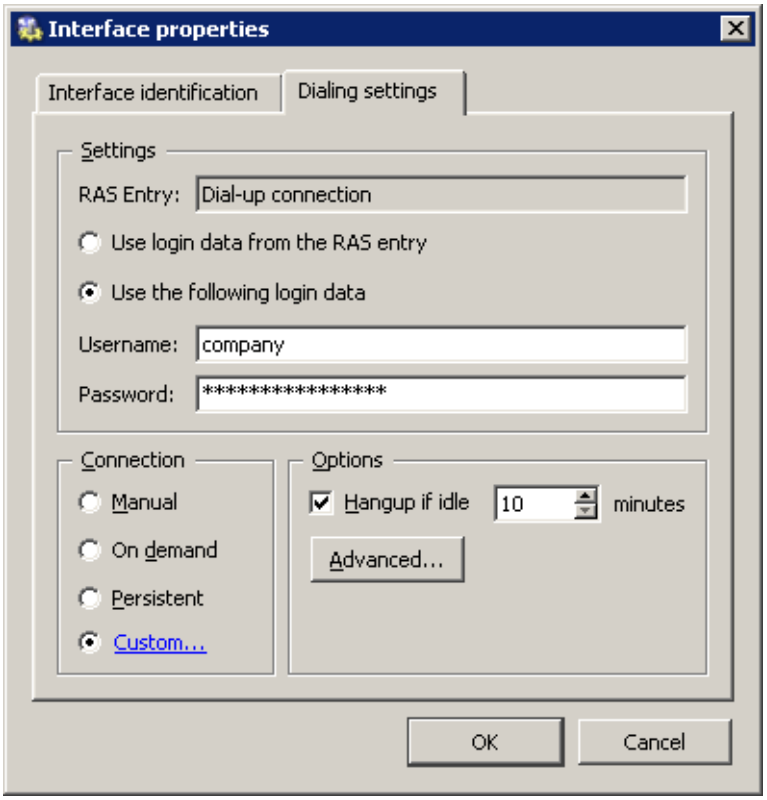


Figure 5.4 Dial-up — dialing parameters

RAS Entry
The Windows *Dial-up Connection* entry that has been selected in the *Interface identification* tab. The name RAS item is displayed for informational purposes.

Use login data from the RAS entry
Enable this option to use login data saved in a corresponding *RAS Entry* configuration for authentication at the remote server.

Use the following login data
Use the *Username* and *Password* entries to enter login data which will be used for authentication at the remote server. This option can be useful for example when for any reason it is not desirable to save the login data in the operating system, when the data is supposed to be edited remotely (via the *Administration Console*) or in case of problem solving.

Connection

Connection type that can be used for dialing:

- *Manual* — the line can only be dialed manually, either from the *Administration Console* or from *WinRoute's* Web interface (see chapter 9).
- *On Demand* — the line will be dialed whenever a host on the LAN tries to access the Internet (incoming packet). To see details about the *WinRoute* and system on-demand dial configuration refer to chapter 16.2.
- *Persistent* — the line will be dialed immediately after the *WinRoute Firewall Engine* service is started and it will be kept active (and will be reconnected if the line is dropped for some reason).
- *Custom* — here you can set with great detail and complexity when the line should be dialed persistently or on demand or not dialed at all.

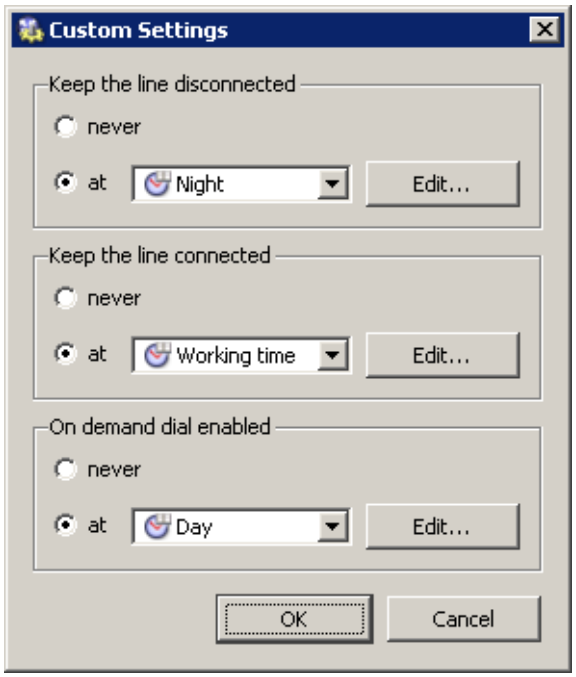


Figure 5.5 Dial-up — demand dial

In sections of the dialog window you can select time ranges for each dialing type. Click on the *Edit* button to open a dialog where time ranges can be created or edited. For more information about time ranges refer to chapter 12.2.
This is how the user defined dialing works:

- The *Keep the line disconnected* option is processed prior to all other options. The line is kept disconnected during this period (or it is hung-up automatically).
- The time range for the *Persistent connection* option is processed as seconds. During this period the line will be kept connected.

- The *On demand dial enabled* option is processed with the lowest priority. If the *always* option is selected, on-demand dial will be allowed anytime when it is not conflicting with the time range of the *never* option.

Hangup if idle

If the line is idle for the period defined, it will be hung up automatically. With each incoming or outgoing packet, the timer of inactivity is set to zero.
There is no such thing as optimum length of the timeout period. If it is too short, the line is dialed too frequently, if too long, the line is kept connected too long. Both increase the Internet connection costs.
Note: This option does not take any effect in case that the connection is set as persistent (or in time ranges where it is set as persistent) — see above.

Advanced

WinRoute allows launching an application or a command in the following situations: *Before dial*, *After dial*, *Before hang-up* or/and *After hang-up*.
Note: In case of the *Before dial* and *Before hang-up* options, the system does not wait for its completion after startup of the program.

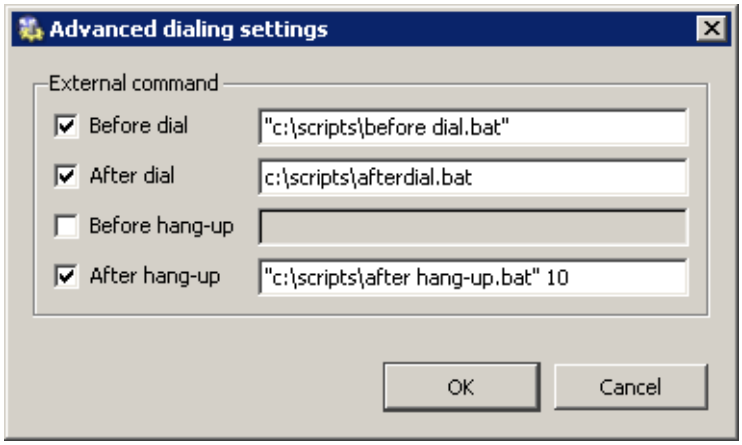


Figure 5.6 Dial-up — external commands

Path to the executable file must be complete. If the path includes spaces it must be closed into quotes, otherwise the part after a space will be considered as a parameter(s) of a batch file. If the path to the file is quoted, the text which follows the closing quote mark is also considered as batch file parameter(s).
Warning: WinRoute is running in the operating system as a service. Therefore, external applications and operating system's commands will run in the background only (within the *SYSTEM* account). The same rules are applied for all external commands and external programs called by scripts. Therefore, it is not highly unrecommended to use interactive applications (i.e. applications with user interaction) for the actions described above. Otherwise. interactive applications are running as "invisible" until the next reboot or until the particular process is ended by the

Windows Task Manager. Under specific circumstances, such application might also block other dials or hang-ups.

Edit Interface parameters

Click *Edit* to modify parameters of a selected interface. The *Interface properties* dialog, identical with the dialog for adding of a new RAS dial-up, is opened in case of RAS dial-ups. Only the *Interface name* entry can be edited in case of network adapters.

For *VPN server* and VPN tunnels, a dialog for setting of the *VPN server* (see chapter 21.1) or a VPN tunnel (refer to chapter 21.3) will be opened.

5.2 Connection Failover

WinRoute allows for definition of connection failover (secondary connection). This secondary connection is enabled automatically whenever a dropout of the primary Internet connection is detected. Functionality of the primary connection is tested by sending of *ICMP Echo Requests* (*PING*) to selected computers. When *WinRoute* finds out that the primary connection is recovered again, the secondary connection is disabled and the primary one is established automatically.

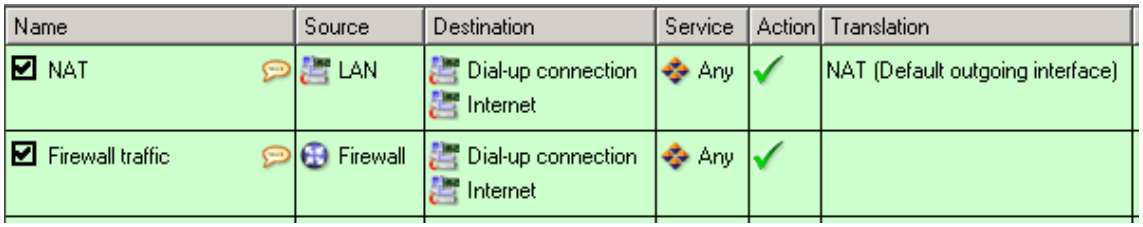
Any network interface or dial connection defined in *WinRoute* can be used as an secondary connection (see chapter 5.1). Traffic rules permitting or denying relevant communication through the secondary connection must be defined. In other words, it is necessary to add an interface for secondary connection to each rule where an interface for primary connection is included in the *Source* or/and *Destination* column.

For detailed information about traffic rules, refer to chapter 6.3.

Example: Primary connection used for traffic going out to the Internet is performed by a network adapter (labeled as *Internet* in *WinRoute*). A *Dial-up Connection* interface will be used for the secondary connection. We want to deny the *Telnet* service in direction from the local network to the Internet.

This situation is shown by traffic rules at figure 5.7. Two destination items are specified for each rule: network connected to the *Internet* interface (primary connection) and network connected to the *Dial-up Connection* interface (secondary connection).

- *NAT* — translation of source IP addresses will be performed for connections from the local network to the Internet (shared Internet connection).
- *Firewall traffic* — the *WinRoute* host will be allowed to connect to the Internet (NAT is not necessary since this host has its proper IP address).



Name	Source	Destination	Service	Action	Translation
NAT	LAN	Dial-up connection Internet	Any	✓	NAT (Default outgoing interface)
Firewall traffic	Firewall	Dial-up connection Internet	Any	✓	

Figure 5.7 Traffic policy for primary and alternative Internet connections

Notes:

1. Traffic rules must be defined by the moment when Connection Failover Setup (see below) is enabled, otherwise the connection will not function properly.

2. Use the *Default outgoing interface* option in the *NAT* rule to ensure that the source IP address in packets going from the local network to the Internet is always resolved to the appropriate IP address (i.e. to the IP address of either the primary or secondary interface — accordingly to which one is used at that moment).

   To specify an IP address for NAT, two independent rules must be defined — one for the primary and the other for an secondary connection.

Connection Failover Setup

Use the *Connection failover* tab in *Configuration* → *Interfaces* to define a secondary connection.

Enable automatic connection failover

Use this option to enable/disable connection failover.

Current connection

This item informs users on which connection is currently active:

- *Primary* connection — in a green field
- *Secondary* connection — in a purple field

Note: Current connections can be switched any time. To view the current status click on the *Refresh* button (at the bottom of the *Connection failover* tab).

Probe hosts

In this section, it is necessary to specify at least one computer (or router, etc.) the availability of which will be tested by *WinRoute* in regular intervals.
The simplest method is to use the default gateway of the primary connection as the testing computer. If the default gateway is not available, the Internet connection is not working (correctly).
If the default gateway cannot be used as the testing computer by any reason, it is possible to use IP addresses of one or more testing computers. If at least one of the tested devices is available, the primary connection is considered as functioning.

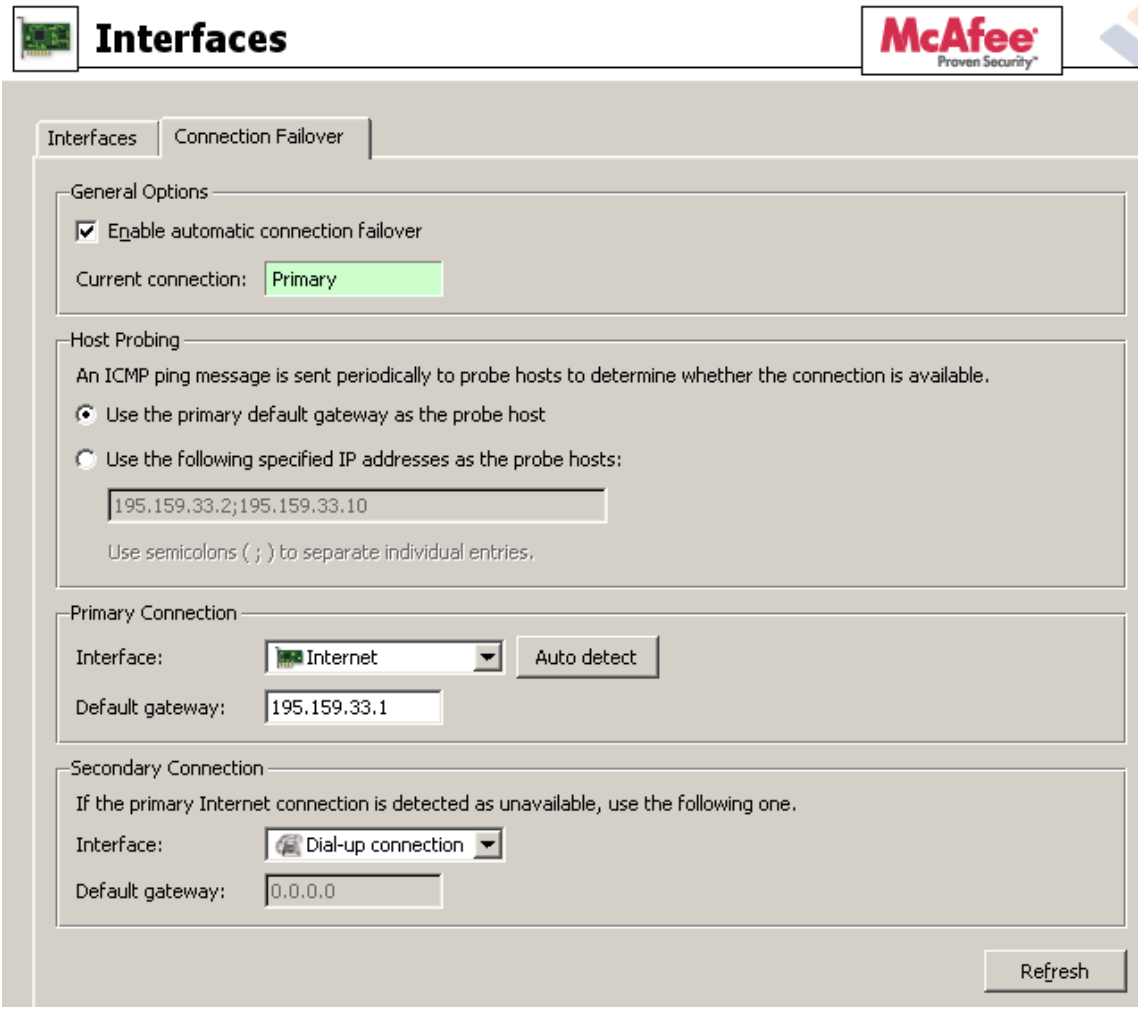


Figure 5.8 Configuration of primary and secondary Internet connection

Notes:

1. Connection failover is enabled only if at least one probe host is specified (*WinRoute* is not able to detect fails of the primary connection unless at least one probe host is defined).
2. Probe hosts must be represented by computers or network devices which are permanently running (servers, routers, etc.). Workstations which are running only a few hours per day are irrelevant as probe hosts.
3. Probe hosts must not block *ICMP Echo Requests* (*PING*) since such requests are used to test availability of these hosts — otherwise the hosts will be always considered as unavailable. This is one of the cases where the primary default gateway cannot be used as the testing computer.

Primary connection

Parameters of the primary Internet connection. The connection can be defined as follows:

- network interface with a default gateway
- dial-up connection

Only interfaces and dial-up connections defined through the *Interfaces* tab are available in the *Interface* entry (see chapter 5.1).

Default settings (default gateway and a corresponding interface) are detected in the operating system after *WinRoute* installation, or when the *Enable automatic connection failover* option is enabled the first time. This can be also be achieved by clicking on the *Detect* button.

If no default gateway is defined in the operating system (i.e. when the primary connection is performed by a dial-up which is currently hung-up), a primary connection cannot be detected automatically — the primary connection must be set by hand.

Secondary connection

Use this section to set parameters for a secondary Internet connection which will be established in case that a primary connection dropout is detected. The secondary connection can be defined as a network interface with a default gateway or as a dial-up connection (like for the primary connection).

Note: The same adapter as for the primary connection can be used, however, the default gateway must be different. This way we can be sure that a different router in the same network (subnet) will be used when the primary connection is dropped out.

Dial-up Use

The following issues must be taken into consideration if a dial-up is used for the primary and/or the secondary connection:

1. Connection failover is relevant only if performed by a permanent connection (using a network adapter or a permanently connected dial-up). If an on-demand dial-up (or a dial-up connection dialed by hand) was used for the primary connection, the secondary connection would be established automatically after each hang-up of the primary connection.

2. In case of manually dialed secondary line a problem might occur if the *Hangup if idle* option is enabled. If the secondary line is hung-up automatically, *WinRoute* does not dial it automatically (until the connections are refreshed and the next failure of the primary connection).

For these reasons we recommend you to set dial-up parameters as follows:

- for the primary connection — *persistent connection*,
- for secondary connection — *on-demand dialing* or *manual dialing without an interval set for hanging-up when idle*.

Note: The *Administration Console* checks settings of dial-up lines selected for the primary or secondary connection and displays an alert in the following cases:

- for the primary connection, a line which is not connected persistently is selected,
- for the secondary connection, a line is selected that can be dialed manually and hung-up when idle.

5.3 DNS Forwarder

In *WinRoute*, the *DNS Forwarder* plug-in can be used to enable easier configuration for DNS hosts within local networks or to speed up responses to repeated DNS queries. At local hosts, DNS can be defined by taking the following actions:

- use IP address of the primary or the back-up DNS server. This solution has the risk of slow DNS responses.
- use the DNS server within the local network (if available). The DNS server must be allowed to access the Internet in order to be able to respond even to queries sent from outside of the local domain.
- use *DNS Forwarder* in *WinRoute*. DNS Forwarder can be also used as a basic DNS server for the local domain (see below) or as a forwarder for the existing server.

If possible, it is recommended to use *DNS Forwarder* as a primary DNS server for LAN hosts (the last option). *DNS Forwarder* provides fast processing of DNS requests and their correct routing in more complex network configurations.

DNS Forwarder configuration

In *WinRoute* default settings the *DNS Forwarder* is switched on and set up so that all DNS queries are forwarded by one of the DNS servers defined in the operating system (usually it is a DNS server provided by your ISP). The configuration can be fine-tuned in *Configurations* → *DNS Forwarder*.

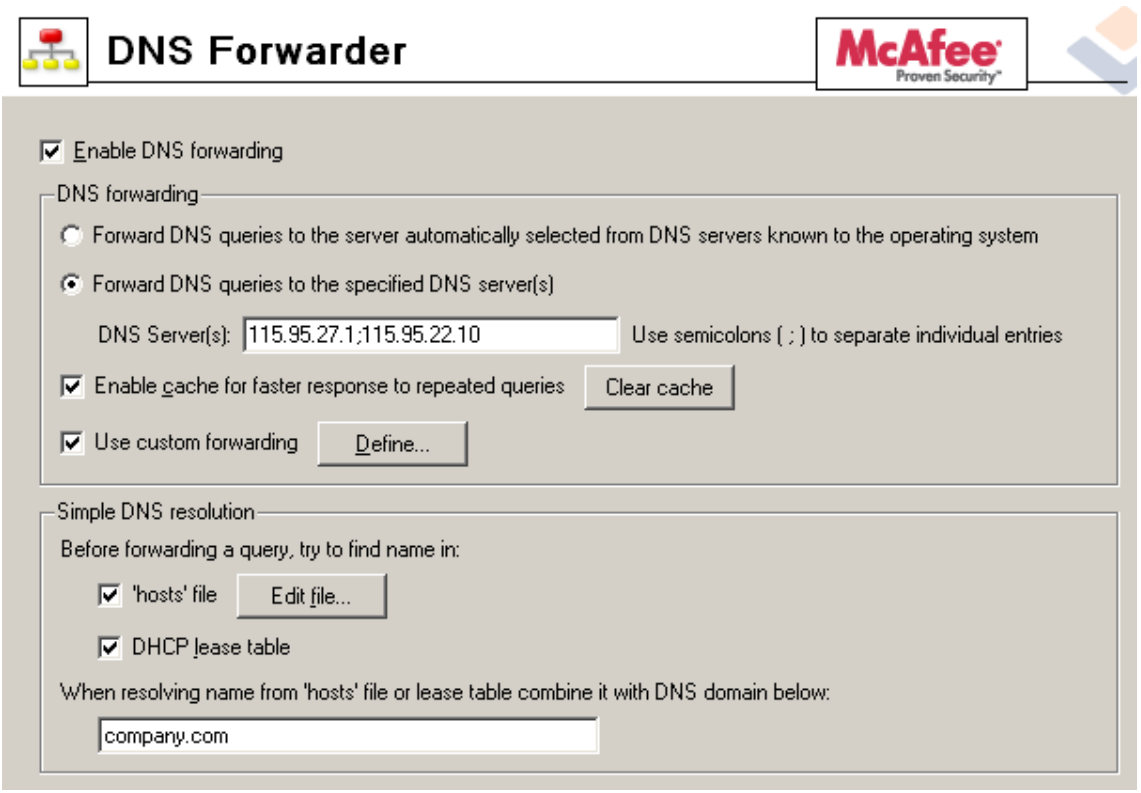

DNS Forwarder
McAfee
Proven Security
Enable DNS forwarding
DNS forwarding
Forward DNS queries to the server automatically selected from DNS servers known to the operating system
Forward DNS queries to the specified DNS server(s)
DNS Server(s): 115.95.27.1;115.95.22.10
Use semicolons (;) to separate individual entries
Enable cache for faster response to repeated queries
Clear cache
Use custom forwarding
Define...
Simple DNS resolution
Before forwarding a query, try to find name in:
'hosts' file
Edit file...
DHCP lease table
When resolving name from 'hosts' file or lease table combine it with DNS domain below:
company.com

Figure 5.9 DNS forwarder settings

Enable DNS forwarding

This option switches between the on/off modes of the *DNS Forwarder* (the service is running on the port 53 and UDP protocol is used by this service). If *DNS Forwarder* is not used for your network configuration, it can be switched off. If you want to run another DNS server on the same host, *DNS Forwarder must* be switched off, or there will be a collision on the port.

DNS forwarding

DNS Forwarder must know at least one DNS server to forward queries to. This option defines how *DNS Forwarder* will identify the IP address of the server:

- *Forward DNS queries to the server automatically...* — functional Internet connection is required. At least one DNS server must be defined within TCP/IP configuration (in Windows, DNS servers are defined at a particular adapter, however, these settings will be used within the entire operating system).
  DNS Forwarder can read these settings and use the same DNS servers. This provides the following benefit — the hosts within the local network and the *WinRoute* host will use the same DNS server.
- *Forward DNS queries to the specified DNS server(s)* — DNS queries will be forwarded to the specified DNS server/servers (if more than one server specified,

they are considered primary, secondary, etc.). This option should be used when there is the need to monitor where DNS queries are forwarded to or to create a more complex configuration.

Enable cache for faster response of repeated queries

If this option is on, all responses will be stored in local *DNS Forwarder* cache. Responses to repeated queries will be much faster (the same query sent by various clients is also considered as a repeated query).

Physically, the DNS cache is kept in RAM. However, all DNS records are also saved in the `DnsCache.cfg` file (see chapter 23.2). This means that records in DNS cache are kept even after *WinRoute Firewall Engine* is stopped or *WinRoute* is disconnected.

Notes:

1. Time period for keeping DNS logs in the cache is specified individually in each log (usually 24 hours).
2. Use of DNS also speeds up activity of the built-in proxy server (see chapter 5.5).

Clear cache

Click this button to remove all records in the *DNS Forwarder's* cache (regardless of their lifetime). This feature can be helpful e.g. for configuration changes, dial-up testing, error detection, etc.

Use custom forwarding

Use this option to enable settings for forwarding certain DNS queries to other DNS servers.

Enable DNS forwarding

DNS forwarder allows forwarding of certain DNS requests to specific DNS servers. Request forwarding is defined by rules for DNS names or subnets. If a DNS name or a subnet in a request matches a rule, the request is forwarded to the corresponding DNS server. Requests matching no rule are forwarded to DNS servers in accordance with settings in the *DNS forwarding* section (see above).

Note: If the simple DNS resolution is enabled (see below), the forwarding rules are applied only if the *DNS Forwarder* is not able to respond by using the information in the *hosts* system file and/or by the DHCP lease table.

DNS forwarding can be helpful for example when we intend to use a local DNS server for the local domain (the other DNS queries will be forwarded to the Internet directly — this will speed up the response). DNS forwarder's settings also play role in configuration of private networks where it is necessary to provide correct forwarding of requests for names in domains of remote subnets (for details, check chapter 21).

Use the *Define* button to open the dialog for definition of DNS forwarding rules.

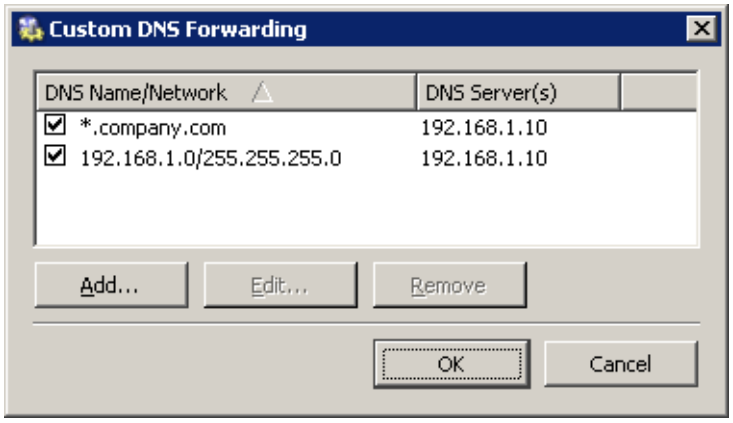


Figure 5.10 Specific settings of DNS forwarding

DNS server can be specified for:

- DNS name — queries requiring names of computers will be forwarded to this DNS server (so called A queries)
- a subnet — queries requiring IP addresses of the particular domain will be forwarded to the DNS server (reverse domain — PTR queries)

Click on the *Add* or the *Edit* button to open a dialog where custom DNS forwarding rules can be defined.

- The *Name DNS query* option allows specification of a rule for name queries. Use the *If the queried name matches* entry to specify a corresponding DNS name (name of a host in the domain).

  It is usually desirable to forward queries to entire domains rather than to specific names. Specification of a domain name may therefore contain * wildcard symbol (asterisk — substitutes any number of characters) and/or ? (question mark — substitutes a single character). The rule will be applied to all names matching with the string (hosts, domains, etc.).

  Example: DNS name will be represented by the string `?erio.c*`. The rule will be applied to all names in domains `kerio.cz`, `cerio.com`, `aerio.c` etc., such as on `www.kerio.cz`, `secure.kerio.com`, `www.aerio.c`, etc.

  Warning: It is necessary that the expression specified in the *If the query contains domain* entry is an entire DNS name! If, for example, the `kerio.c*` expression is introduced, only names `kerio.cz`, `kerio.com` etc. would match the rule and host names included in these domains (such as `www.kerio.cz` and `secure.kerio.com`) would not!

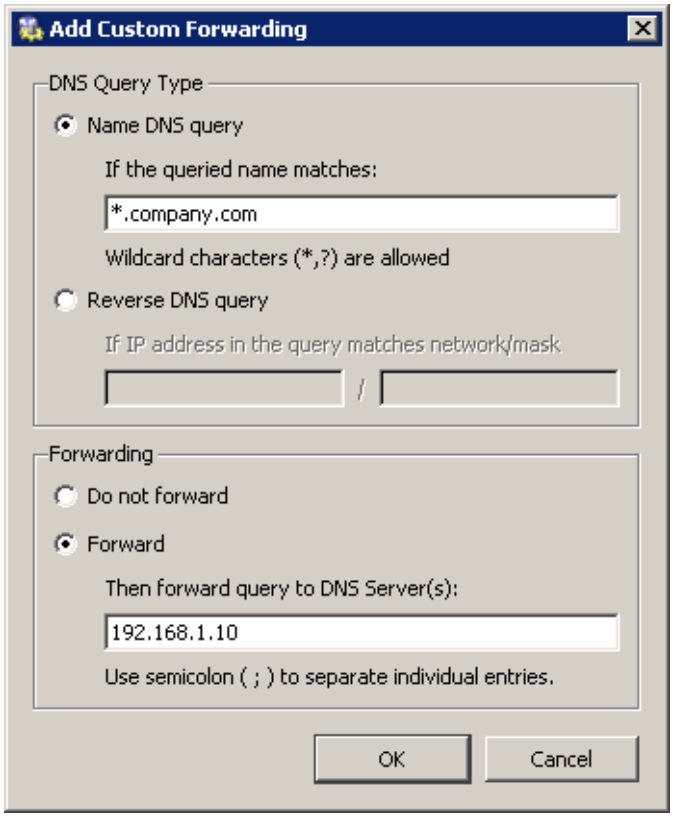


Figure 5.11 DNS forwarding — a new rule

- Use the *Reverse DNS query* alternative to specify rule for DNS queries on IP addresses in a particular subnet. Subnet is specified by a network address and a corresponding mask (i.e. `192.168.1.0 / 255.255.255.0`).

- Use the *Then forward query to DNS Server(s)* field to specify IP address(es) of one or more DNS server(s) to which queries will be forwarded.

  If multiple DNS servers are specified, they are considered as primary, secondary, etc.

  If the *Do not forward* option is checked, DNS queries will not be forwarded to any server — *WinRoute* will search only in the `hosts` local file or in DHCP tables (see below).

Simple DNS resolution

DNS Forwarder can be used as a simple DNS server, typically for a local domain. If the simple DNS resolution is set, the *DNS forwarder* attempts to respond to the received DNS query first and it does not forward it to another DNS server unless unsuccessful.

Before forwarding a query...

These options allow setting of where the *DNS Forwarder* would search for the name or IP address before the query is forwarded to another DNS server.

- *'hosts' file* — this file can be found in any operating system supporting TCP/IP. Each row of this file includes host IP addresses and a list of appropriate DNS names. When any DNS query is received, this file will be checked first to find out whether the desired name or IP address is included. If not, the query is forwarded to a DNS server.
  If this function is on, *DNS Forwarder* follows the same rule. Use the *Edit* button to open a special editor where the `HOSTS` file can be edited via *Administration Console* even if this console is connected to *WinRoute* remotely.

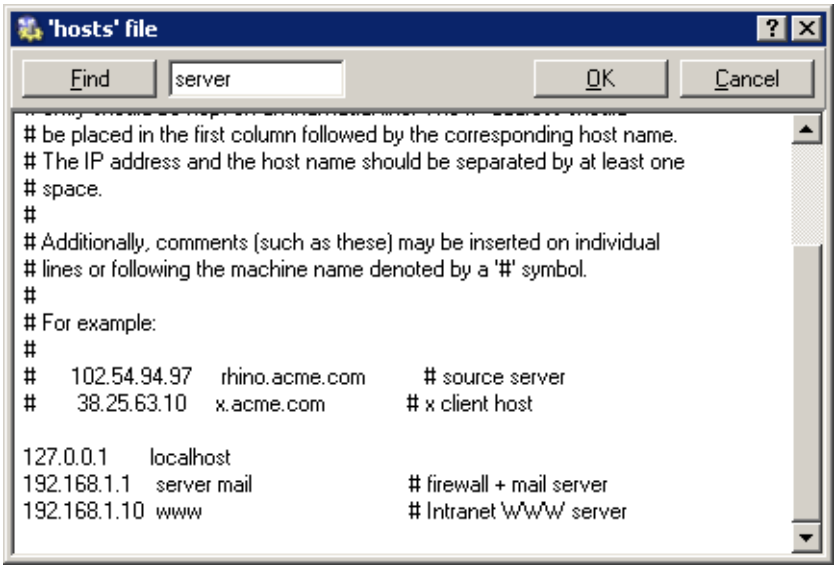

'hosts' file
Find
server
OK
Cancel
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97 rhino.acme.com # source server
38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
192.168.1.1 server mail # firewall + mail server
192.168.1.10 www # Intranet WWW server

Figure 5.12 Editor of the Hosts system file

- *DHCP lease table*— if the hosts within local network are configured by the DHCP server in *WinRoute* (see chapter 5.4), the DHCP server knows what IP address was defined for each host. After starting the system, the host sends a request for IP address definition including the name of the host.
  DNS Forwarder can access DHCP lease tables and find out which IP address has been assigned to the host name. If asked to inform about the local name of the host, *DNS Forwarder* will always respond with the current IP address.

Note: If both options are disabled, the *DNS Forwarder* forwards all queries to other DNS servers.

Combine the name ... with DNS domain

Insert the name of the local DNS domain in this text field.
If a host sends a query to obtain an IP address, it uses the name only (it has not found out the domain yet). *DNS Forwarder* needs to know the name of the local

domain to answer queries on fully qualified local DNS names (names including the domain).
The problem can be better understood through the following example:
The local domain's name is `company.com`. The host called `john` is configured so as to obtain an IP address from the DHCP server. After the operating system is started the host sends to the DHCP server a query with the information about its name (`john`). The DHCP server assigns the host IP address `192.168.1.56`. The DHCP server then keeps the information that the IP address is assigned to the `honza` host.
Another host that wants to start communication with the host will send a query on the `john.company.com` name (the `john` host in the `company.com` domain). If the local domain name would not have been known by *DNS Forwarder*, the forwarder would pass the query to another DNS server as it would not recognize that it is a name from the local domain. However, as *DNS Forwarder* knows the local domain name, the `company.com` name will be separated and the `john` host with the appropriate IP address will be easily looked up in the DHCP table.
Note: If the local domain is specified in *DNS Forwarder*, local names with or without the domain can be recorded in the `HOSTS` system file.

5.4 DHCP server

The DHCP protocol (*Dynamic Host Configuration Protocol*) is used for easy TCP/IP configuration of hosts within the network. Upon an operation system start-up, the client host sends a configuration request that is detected by the DHCP server. The DHCP server selects appropriate configuration parameters (IP address with appropriate subnet mask and other optional parameters, such as IP address of the default gateway, addresses of DNS servers, domain name, etc.) for the client stations. All client parameters can be set at the server only — at individual hosts, enable the option that TCP/IP parameters are configured automatically from the DHCP server. For most operating systems (e.g. Windows, Linux, etc.), this option is set by default — it is not necessary to perform any additional settings at client hosts.

The DHCP server assigns clients IP addresses within a predefined scope for a certain period (*lease time*). If an IP address is to be kept, the client must request an extension on the period of time before the lease expires. If the client has not required an extension on the lease time, the IP address is considered free and can be assigned to another client. This is performed automatically and transparently.

So called reservations can be also defined on the DHCP server — certain clients will have their own IP addresses reserved. Addresses can be reserved for a hardware address (MAC) or a host name. These clients will have fixed IP address. These addresses are configured automatically.

Using DHCP brings two main benefits. First, the administration is much easier than with the other protocols as all settings may be done at the server (it is not necessary to configure individual workstations). Second, many network conflicts are eliminated (i.e. one IP address cannot be assigned to more than one workstation, etc.).

DHCP Server Configuration

To configure the DHCP server in *WinRoute* go to *Configuration* → *DHCP Server*. Here you can define IP scopes, reservations or optional parameters, and view information about occupied IP addresses or statistics of the DHCP server.

The DHCP server can be enabled/disabled using the *DHCP Server enabled* option (at the top). Configuration can be modified even when the DHCP server is disabled.

Definition of Scopes and Reservations

To define scopes including optional parameters and to reserve IP addresses for selected clients go to the *Scopes* dialog. The tab includes two parts — in one address scopes and in the other reservations are defined:

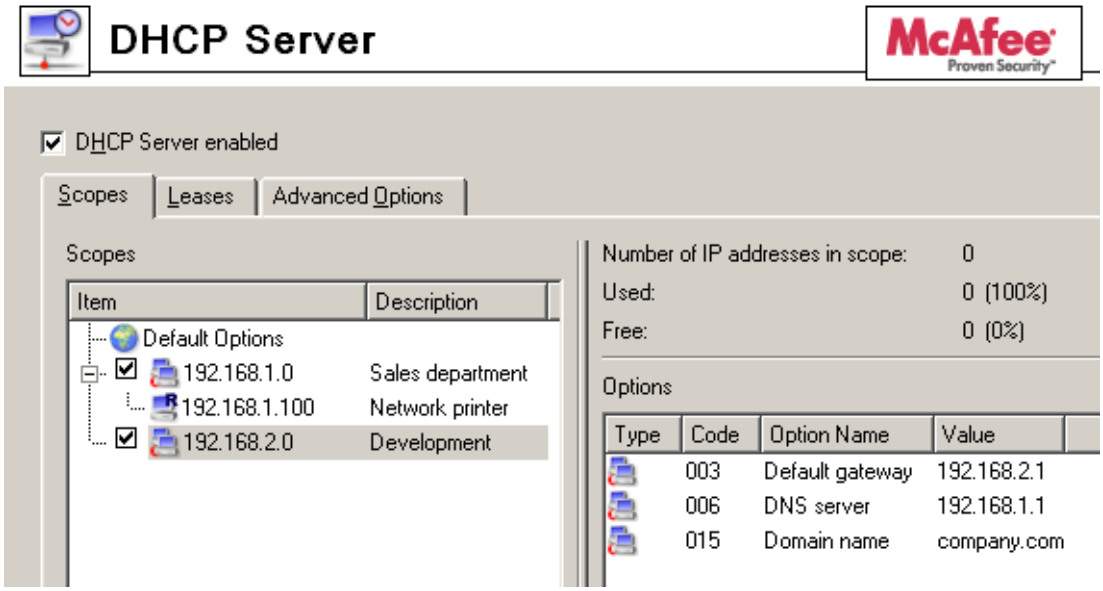


Figure 5.13 DHCP server — IP scopes

In the *Item* column, you can find subnets where scopes of IP addresses are defined. The IP subnet can be either ticked to activate the scope or unticked to make the scope inactive (scopes can be temporarily switched off without deleting and adding again). Each subnet includes also a list of reservations of IP addresses that are defined in it.

In the *Default options* item (the first item in the table) you can set default parameters for DHCP server.

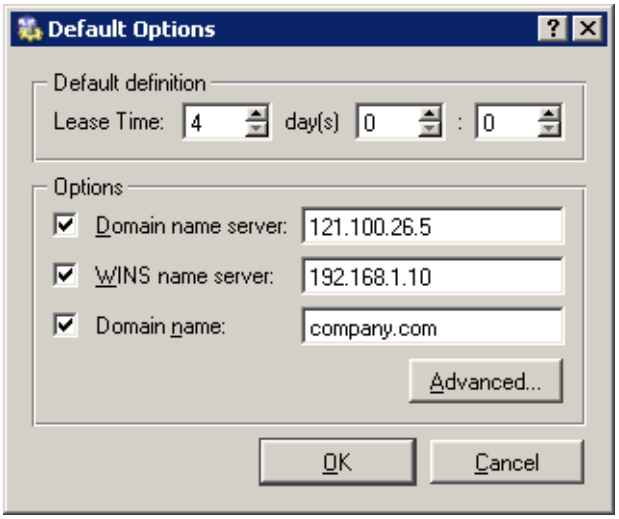


Figure 5.14 DHCP server — default DHCP parameters

Lease time
: Time for which an IP address is assigned to clients. This IP address will be automatically considered free by expiration of this time (it can be assigned to another client) unless the client requests lease time extension or the address release.

DNS server
: Any DNS server (or multiple DNS servers separated by semicolons) can be defined. We recommend you to use *DNS Forwarder* in *WinRoute* as the primary server (first in the list) — IP address of the *WinRoute* host. *DNS Forwarder* can cooperate with DHCP server (see chapter 5.3) so that it will always use correct IP addresses to response to requests on local host names.

WINS server
: IP address of the WINS server.

Domain
: Local Internet domain. Do not specify this parameter if there is no local domain.

Advanced

Click on this button to open a dialog with a complete list of advanced parameters supported by DHCP (including the four mentioned above). Any parameter supported by DHCP can be added and its value can be set within this dialog.

Default parameters are automatically matched with address scopes unless configuration of a particular scope is defined (the *Address Scope* → *Options* dialog). The same rule is applied on scopes and reservations (parameters defined for a certain address scope are used for the other reservations unless parameters are defined for a specific reservation). Weight of individual parameters corresponds with their position in the tree hierarchy.

Select the *Add* → *Scope* option to view the dialog for address scope definition.

Note: Only one scope can be defined for each subnet.

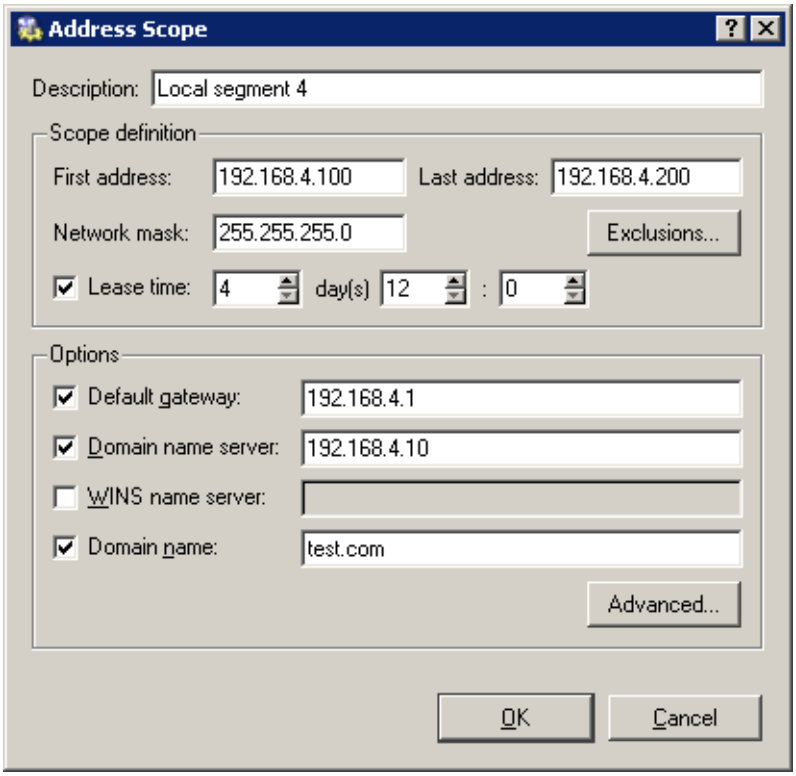


Figure 5.15 DHCP server — IP scopes definition

Description

Comment on the new address scope (just as information for *WinRoute* administrator).

First address, Last address

First and last address of the new scope.

Note: If possible, we recommend you to define the scope larger than it would be defined for the real number of users within the subnet.

Subnet mask

Mask of the appropriate subnet. It is assigned to clients together with the IP address.

Note: The *Administration Console* application monitors whether first and last address belong to the subnet defined by the mask. If this requirement is not met, an error will be reported after the confirmation with the *OK* button.

Lease time

Time for which an IP address is assigned to clients. This IP address will be automatically considered free by expiration of this time (it can be assigned to another client) unless the client requests lease time extension or the address release.

Exclusions

WinRoute enables the administrator to define only one scope in within each subnet. To create more individual scopes, follow these instructions:

- create address scope covering all desired scopes
- define so called exclusions that will not be assigned

Example: In `192.168.1.0` subnet you intend to create two scopes: from `192.168.1.10` to `192.168.1.49` and from `192.168.1.61` to `192.168.1.100`. Addresses from `192.168.1.50` to `192.168.1.60` will be left free and can be used for other purposes.

Create the scope from `192.168.1.10` to `192.168.1.100` and click on the *Exclusions* button to define the scope from `192.168.1.50` to `192.168.1.60`. These addresses will not be assigned by the DHCP server.

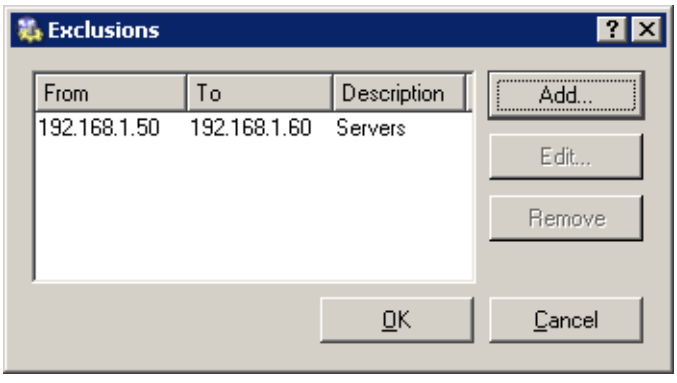


Figure 5.16 DHCP server — IP scopes exceptions

Parameters

In the *Address Scope* dialog, basic DHCP parameters of the addresses assigned to clients can be defined:

- *Default Gateway* — IP address of the router that will be used as the default gateway for the subnet from which IP addresses are assigned. IP address of the interface the network is connected to. Default gateway of another network would be useless (not available to clients).
- *DNS server* — any DNS server (or more DNS servers separated with semicolons). We recommend you to use *DNS Forwarder* in *WinRoute* as the primary server (first in the list) — IP address of the *WinRoute* host. *DNS Forwarder* can cooperate with DHCP server (see chapter 5.3) so that it will always use correct IP addresses to response to requests on local host names.
- *WINS server*
- *Domain* — local Internet domain. Do not specify this parameter if there is no local domain.
  Warning: This parameter is not used for specification of the name of Windows NT domain!

Advanced

Click on this button to open a dialog with a complete list of advanced parameters supported by DHCP (including the four mentioned above). Any parameter supported by DHCP can be added and its value can be set within this dialog. This dialog is also a part of the *Address Scopes* tab.

To view configured DHCP parameters and their values within appropriate IP scopes see the right column in the *Address Scope* tab.

Note: Simple DHCP server statistics are displayed at the right top of the *Address Scope* tab. Each scope is described with the following items:

- total number of addresses within this scope
- number and percentage proportion of leases
- number and percentage proportion of free addresses

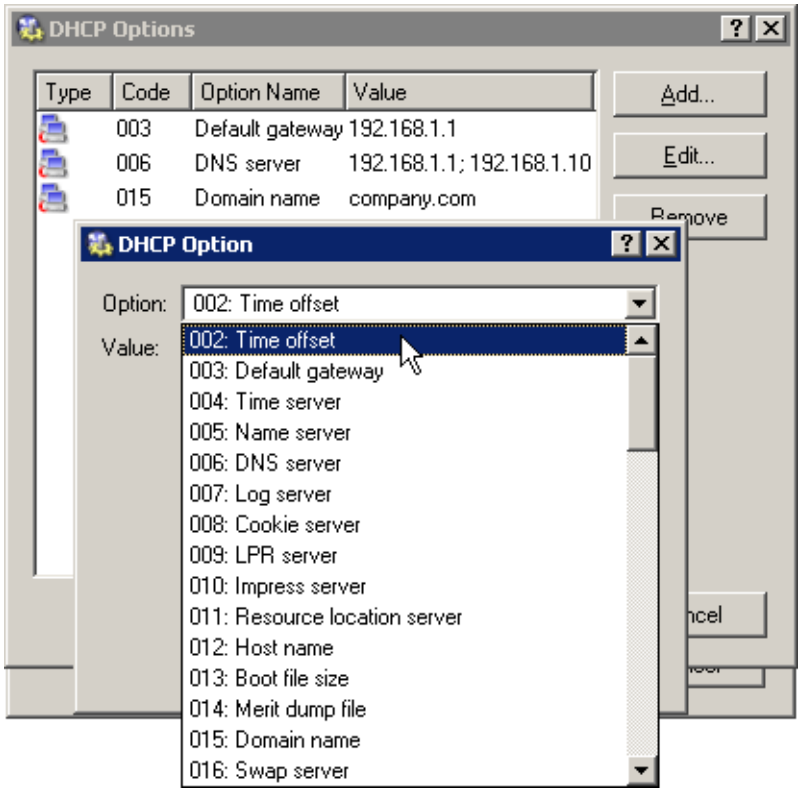


Figure 5.17 DHCP server — DHCP settings

Number of IP's in scope:	90
Used:	86 (96%)
Free:	4 (4%)

Figure 5.18 DHCP server — statistics (leased and free IP addresses within the scope)

Lease Reservations

DHCP server enables the administrator to book an IP address for any host. To make the reservation click on the *Add* → *Reservations* button in the *Scopes* folder.

Any IP address included in a defined subnet can be reserved. This address can but does not have to belong to the scope of addresses dynamically leased, and it can also belong to any scope used for exceptions.

IP addresses can be reserved for:

- hardware (MAC) address of the host — it is defined by hexadecimal numbers separated by colons, i.e.

  `00:bc:a5:f2:1e:50`

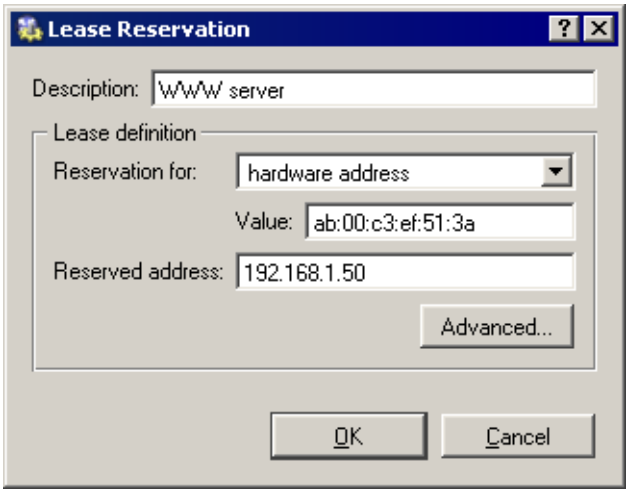


Figure 5.19 DHCP server — reserving an IP address

or by dashes— for example:

`00-bc-a5-f2-1e-50`

The MAC address of a network adapter can be detected with operating system tools (i.e. with the `ipconfig` command) or with a special application provided by the network adapter manufacturer.

- host name — DHCP requests of most DHCP clients include host names (i.e. all Windows operating systems), or the client can be set to send a host name (i.e. Linux operating system).

Click *Advanced* to set DHCP parameters which will accompany the address when leased. If the IP address is already included to a scope, DHCP parameters belonging to the scope are used automatically. In the *Lease Reservation* dialog window, additional parameters can be specified or/and new values can be entered for parameters yet existing.

Note: Another way to reserve an IP address is to go to the *Leases* tab, find the IP address leased dynamically to the host and reserve it (for details, see below).

Leases

IP scopes can be viewed in the *Leases* tab. These scopes are displayed in the form of trees. All current leases within the appropriate subnet are displayed in these trees.

Note: Icon color represents address status (see below). Icons marked with `R` represent reserved addresses.

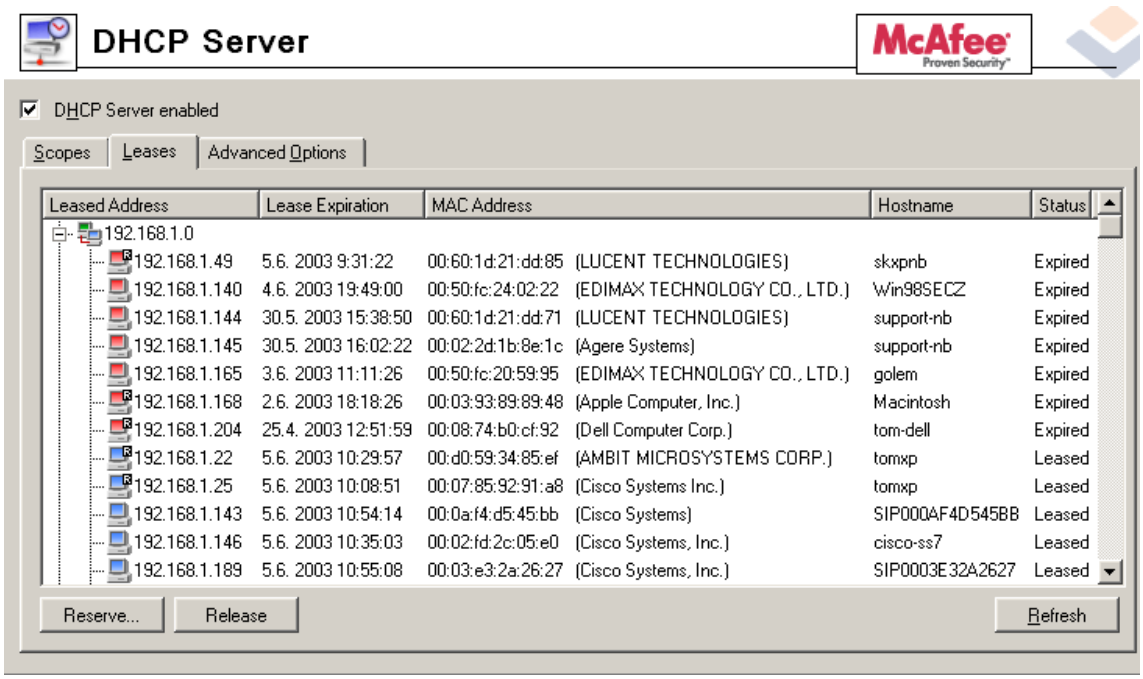

DHCP Server
McAfee
Proven Security
DHCP Server enabled
Scopes
Leases
Advanced Options
Leased Address
Lease Expiration
MAC Address
Hostname
Status
192.168.1.0
192.168.1.49 5.6. 2003 9:31:22 00:60:1d:21:dd:85 (LUCENT TECHNOLOGIES) skxpnb Expired
192.168.1.140 4.6. 2003 19:49:00 00:50:fc:24:02:22 (EDIMAX TECHNOLOGY CO., LTD.) Win98SECZ Expired
192.168.1.144 30.5. 2003 15:38:50 00:60:1d:21:dd:71 (LUCENT TECHNOLOGIES) support-nb Expired
192.168.1.145 30.5. 2003 16:02:22 00:02:2d:1b:8e:1c (Agere Systems) support-nb Expired
192.168.1.165 3.6. 2003 11:11:26 00:50:fc:20:59:95 (EDIMAX TECHNOLOGY CO., LTD.) golem Expired
192.168.1.168 2.6. 2003 18:18:26 00:03:93:89:89:48 (Apple Computer, Inc.) Macintosh Expired
192.168.1.204 25.4. 2003 12:51:59 00:08:74:b0:cf:92 (Dell Computer Corp.) tom-dell Expired
192.168.1.22 5.6. 2003 10:29:57 00:d0:59:34:85:ef (AMBIT MICROSYSTEMS CORP.) tomxp Leased
192.168.1.25 5.6. 2003 10:08:51 00:07:85:92:91:a8 (Cisco Systems Inc.) tomxp Leased
192.168.1.143 5.6. 2003 10:54:14 00:0a:f4:d5:45:bb (Cisco Systems) SIP000AF4D545BB Leased
192.168.1.146 5.6. 2003 10:35:03 00:02:fd:2c:05:e0 (Cisco Systems, Inc.) cisco-ss7 Leased
192.168.1.189 5.6. 2003 10:55:08 00:03:e3:2a:26:27 (Cisco Systems, Inc.) SIP0003E32A2627 Leased
Reserve...
Release
Refresh

Figure 5.20 DHCP server — list of leased and reserved IP addresses

Columns in this section contain the following information:

- *Leased Address* — leased IP address
- *Lease Expiration* — date and time specifying expiration of the appropriate lease
- *MAC Address* — hardware address of the host that the IP address is assigned to (including name of the network adapter manufacturer).
- *Hostname* — name of the host that the IP address is assigned to (only if the DHCP client at this host sends it to the DHCP server)
- *Status* — status of the appropriate IP address; *Leased* (leased addresses), *Expired* (addresses with expired lease — the client has not asked for the lease to be extended yet), *Declined* (the lease was declined by the client) or *Released* (the address has been released by the client).

  Notes:

  1. Data about expired and released addresses are kept by the DHCP server and can be used later if the same client demands a lease. If free IP addresses are lacked, these addresses can be leased to other clients.

  2. Declined addresses are handled according to the settings in the *Options* tab (see below).

The following columns are hidden by default:

- *Last Request Time* — date and time when the recent request for a lease or lease extension was sent by a client
- *Lease Remaining Time* — time remaining until the appropriate *Lease Expiration*

Use the *Release* button to release a selected IP address immediately (independently of its status). Released addresses are considered free and can be assigned to other clients immediately.

Click on the *Reserve* button to reserve a selected (dynamically assigned) IP address based on the MAC address or name of the host that the address is currently assigned to. The *Scopes* tab with a dialog where the appropriate address can be leased will be opened automatically. All entries except for the *Description* item will be already defined with appropriate data. Define the *Description* entry and click on the *OK* button to assign a persistent lease for the IP address of the host to which it has been assigned dynamically.

Note: The MAC address of the host for which the IP is leased will be inserted to the lease reservation dialog automatically. To reserve an IP address for a hostname, change settings of the *Reservation For* and *Value* items.

DHCP server — advanced options

Other DHCP server parameters can be set in the *Options* tab.

BOOTP

If this option is enabled, the DHCP server will assign IP addresses (including optional parameters) also to clients of BOOTP protocol (protocol used formerly to DHCP— it assigns configurations statically only, according to MAC addresses).

Windows RAS

Through this option you can enable DHCP service for RAS clients (Remote Access Service). You can also specify time when the service will be available to RAS clients (an IP address will be assigned) if the default value is not convenient.
Warning:

1. DHCP server cannot assign addresses to RAS clients connecting to the RAS server directly at the *WinRoute* host (for technical reasons, it is not possible to receive DHCP queries from the local RAS server). For such cases, it is necessary to set assigning of IP addresses in the RAS server configuration.
2. The RAS service in Windows leases a new IP address for each connection (even if requested by the same client). *WinRoute* includes RAS clients in total number of clients when checking whether number of licensed users has been exceeded (see chapter 4.6). This implies that repeated connection of RAS clients may

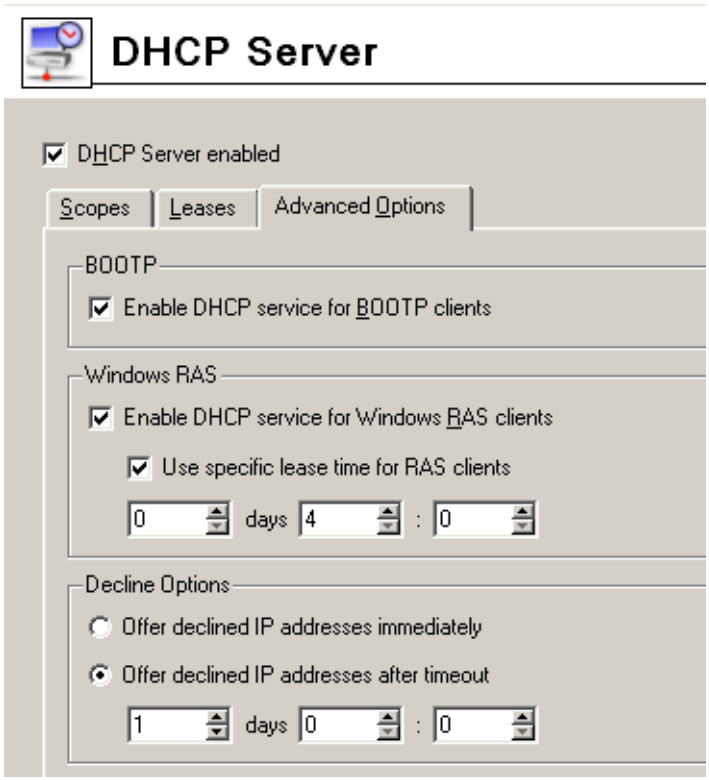


Figure 5.21 DHCP server — advanced options

cause exceeding of the number of licensed users (if the IP scope for the RAS service is too large or/and an address is leased to RAS clients for too long time). Remote clients will be then allowed to connect and communicate with hosts in the local network, while they will not be allowed to connect to the Internet via *WinRoute*.

Declined options

These options define how declined IP addresses (*DHCPDECLINE* report) will be handled. These addresses can be either considered released and assigned to other users if needed (the *Offer immediately* option) or blocked during a certain time for former clients to be able to use them (the *Declined addresses can be offered after timeout* option).

5.5 Proxy server

Even though the NAT technology used in *WinRoute* enables direct access to the Internet from all local hosts, it contains a standard HTTP proxy server. Under certain conditions the direct access cannot be used or it is inconvenient . The following list describes the

most common situations:

1. To connect from the *WinRoute* host it is necessary to use the proxy server of your ISP.

   Proxy server included in *WinRoute* can forward all queries to so called *parent proxy server*).

2. Internet connection is performed via a dial-up and access to certain Web pages is blocked (refer to chapter 10.2). If a direct connection is used, the line will be dialed before the HTTP query could be detected (line is dialed upon a DNS query or upon a client's request demanding connection to a Web server). If a user connects to a forbidden Web page, *WinRoute* dials the line and blocks access to the page — the line is dialed but the page is not opened.

   Proxy server can receive and process clients' queries locally. The line will not be dialed if access to the requested page is forbidden.

3. *WinRoute* is deployed within a network with many hosts where proxy server has been used. It would be too complex and time-consuming to re-configure all the hosts.

   The Internet connection functionality is kept if proxy server is used — it is not necessary to edit configuration of individual hosts (or only some hosts should be re-configured).

The *WinRoute's* proxy server can be used for HTTP, HTTPS and FTP protocols. Proxy server does not support the SOCKS protocol (a special protocol used for communication between the client and the proxy server).

Note: For detailed information on using FTP on the *WinRoute's* proxy server, refer to chapter 23.6.

Proxy Server Configuration

To configure proxy server parameters open the *Proxy server* tab in *Configuration* → *Content Filtering* → *HTTP Policy*.

Enable non-transparent proxy server

This option enables the HTTP proxy server in *WinRoute* on the port inserted in the *Port* entry (3128 port is set by the default).
Warning : If you use a port number that is already used by another service or application, *WinRoute* will accept this port, however, the proxy server will not be able to run and the following report will be logged into the *Error* log (refer to chapter 20.8):

```
failed to bind to port 3128:  another application is using this
port
```

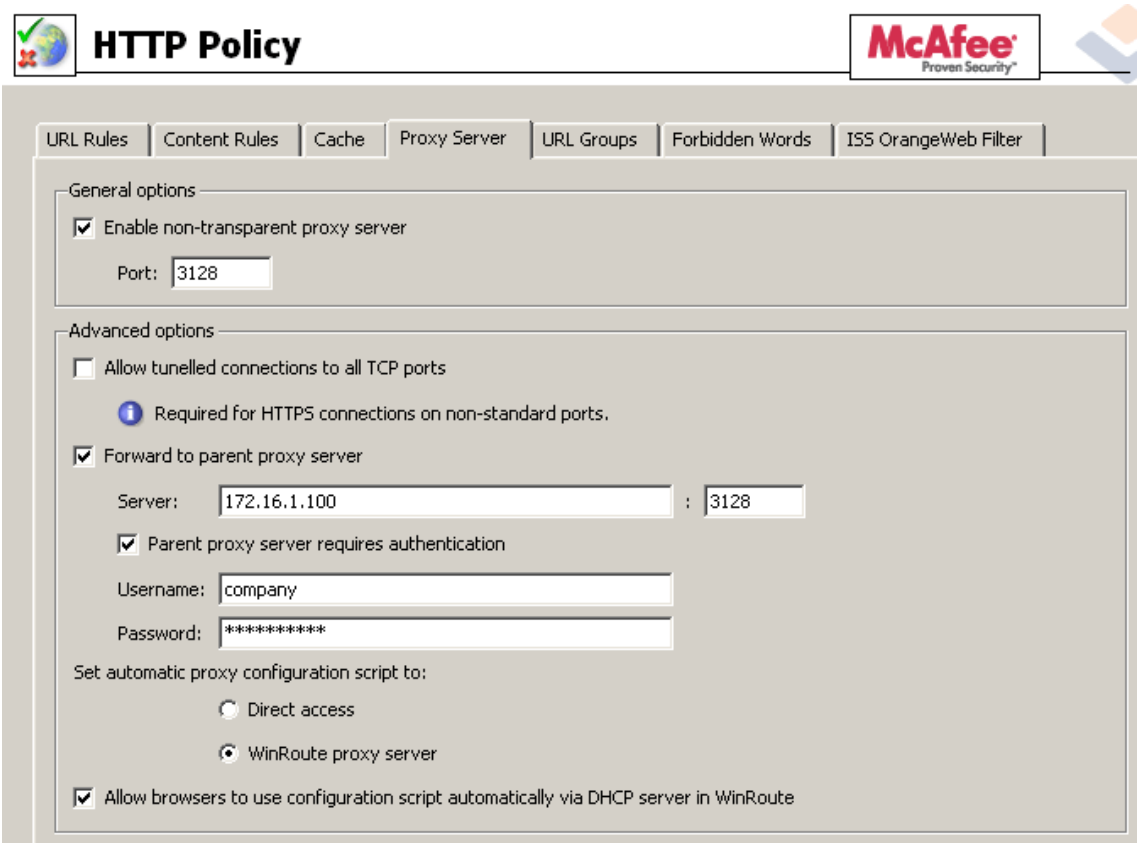


Figure 5.22 HTTP proxy server settings

If you are not sure that the port you intend to use is free, click on the *Apply* button and check the *Error* log (check whether the report has or has not been logged) immediately.

Enable connection to any TCP port

This security option enables to allow or block so called tunneling of other application protocols (than HTTP, HTTPS and FTP) via the proxy server.

If this option is disabled, the proxy server allows to establish connection only to the standard HTTPS port 443) — it is supposed that secured web pages are being opened. If the option is enabled, the proxy server can establish connection to any port. It can be a non-standard HTTPS port or tunneling of another application protocol.

Note: This option does not affect the non-secured traffic performed by HTTP and/or FTP. In *WinRoute*, HTTP traffic is controlled by a protocol inspectors which allows only valid HTTP and FTP queries.

Forward to parent proxy server

Tick this option for *WinRoute* to forward all queries to the parent proxy server which will be specified by the following data:

- *Server* — DNS name or IP address of parent proxy server and the port on which the server is running (`3128` port is used by the default).
- *Parent proxy server requires authentication* — enable this option if authentication by username and password is required by the parent proxy server. Specify the *Username* and *Password* login data.
  Note: The name and password for authentication to the parent proxy server is sent with each HTTP request. Only *Basic* authentication is supported.

The *Forward to parent proxy server* option specifies how *WinRoute* will connect to the Internet (for update checks, downloads of *McAfee* updates and for connecting to the online *ISS OrangeWeb Filter* databases).

Set automatic proxy configuration script to

If a proxy server is used, Web browsers on client hosts must be configured correctly. Most common Web browsers (e.g. *Microsoft Internet Explorer*, *Firefox/Netscape/Mozilla/SeaMonkey*, *Opera*, etc.) enable automatic configuration of corresponding parameters by using a script downloaded from a corresponding Website specified with URL.
In the case of *WinRoute's* proxy server, the configuration script is saved at

`http://192.168.1.1:3128/pac/proxy.pac,`

where `192.168.1.1` is the IP address of the *WinRoute* host and number `3128` represents the port of the proxy server (see above).
The *Allow browsers to use configuration script automatically...* option adjusts the configuration script in accord with the current *WinRoute* configuration and the settings of the local network:

- *Direct access* — no proxy server will be used by browsers
- *WinRoute proxy server* — IP address of the *WinRoute* host and the port on which the proxy server is running will be used by the browser (see above).

Note: The configuration script requires that the proxy server is always available (even if the *Direct access* option is used).

Allow browsers to use configuration script automatically...

It is possible to let *Microsoft Internet Explorer* be configured automatically by the DHCP server. To set this, enable the *Automatically detect settings* option.
WinRoute's DHCP server must be running (see chapter 5.4), otherwise the function will not work. TCP/IP parameters at the host can be static — *Microsoft Internet Explorer* sends a special DHCP query when started.
HINT: This method enables to configure all *Microsoft Internet Explorer* browsers at

all local hosts by a single click.

5.6 HTTP cache

Using cache to access Web pages that are opened repeatedly reduces Internet traffic (in case of line where traffic is counted, it is also remarkable that using of cache decreases total volume of transferred data). Downloaded files are saved to the harddisk of the *WinRoute* host so that it is not necessary to download them from the Web server again later.

All objects are stored in cache for a certain time only (*Time To Live — TTL*). This time defines whether checks for the most recent versions of the particular objects will be performed upon a new request of the page. The required object will be found in cache unless the *TTL* timeout has expired. If it has expired, a check for a new update of the object will be performed. This ensures continuous update of objects that are stored in the cache.

The cache can be used either for direct access or for access via the proxy server. If you use direct access, the HTTP protocol inspector must be applied to the traffic. In the default configuration of *WinRoute*, this condition is met for the HTTP protocol at the default port 80 (for details, see chapters 6.3 and 12.3).

To set HTTP cache parameters go to the *Cache* tab in *Configuration* → *Content Filtering* → *HTTP Policy*.

Enable cache on transparent proxy
: This option enables cache for HTTP traffic that uses the HTTP protocol inspector (direct access to the Internet).

Enable cache on proxy server
: Enables the cache for HTTP traffic via *WinRoute's* proxy server (see chapter 5.5).

HTTP protocol TTL
: Default time of object validity within the cache. This time is used when:

- TTL of a particular object is not defined (to define TTL use the *URL specific settings* button —see below)
- TTL defined by the Web server is not accepted (the *Use server supplied Time-To-Live* entry)

Cache directory
: Directory that will be used to store downloaded objects. The `cache` file under the directory where *WinRoute* is installed is used by default.
Warning: Changes in this entry will not be accepted unless the *WinRoute Firewall Engine* is restarted. Old cache files in the original folder will be removed automatically.

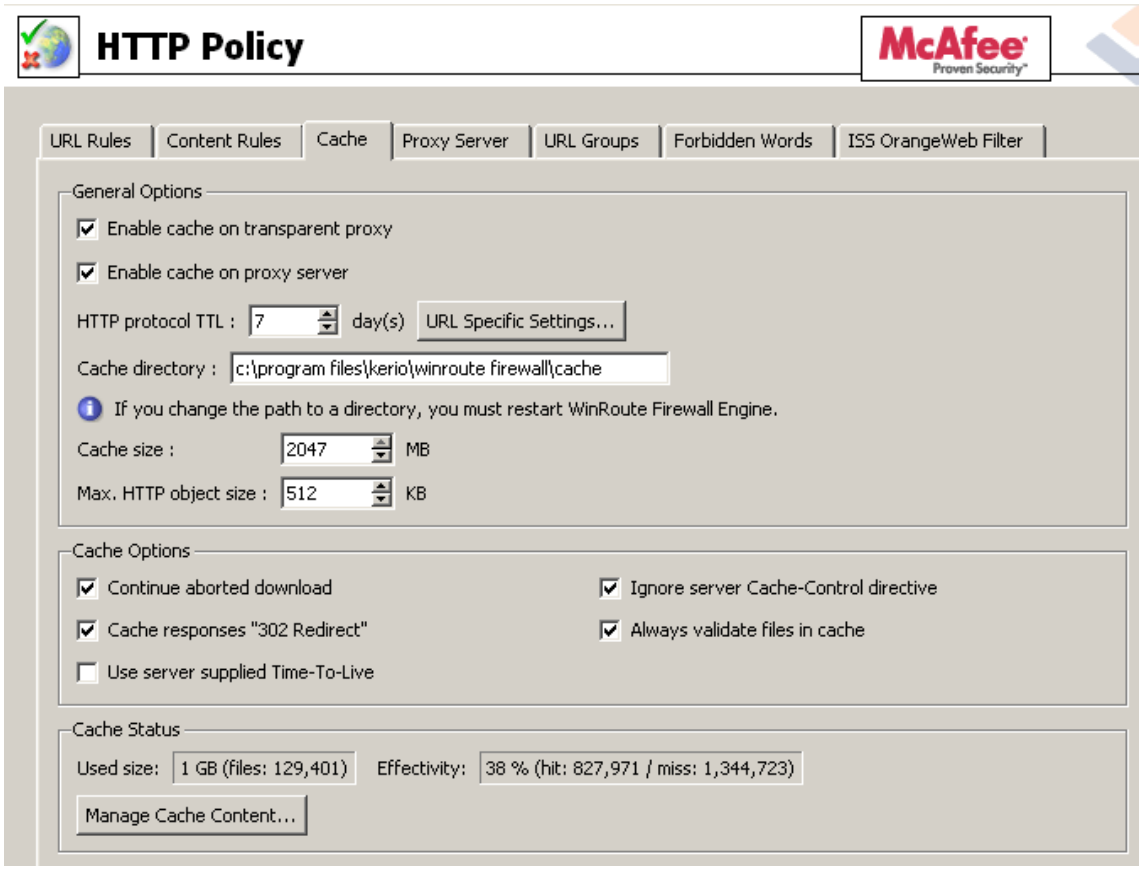


Figure 5.23 HTTP cache configuration

Cache size

Size of the cache file on the disk. Maximal cache size allowed is *2 GB* (*2047 MB*)
Notes:

1. If 98 per cent of the cache is full, a so called cleaning will be run — this function will remove all objects with expired TTL. If no objects are deleted successfully, no other objects can be stored into the cache unless there is more free space on the disk (made by further cleaning or by manual removal).
2. The maximal cache size is applied in *WinRoute* since *6.2.0*. In older versions, maximal cache size allowed was *4 GB* (the treshold was cut for technical reasons). If, upon its startup, the *WinRoute Firewall Engine* detects that the cache size exceeds *2047 MB*, the size is changed to the allowed value automatically.
3. If the maximum cache size set is larger than the free space on the corresponding disk, the cache is not initialized and the following error is recorded in the *Error* log (see chapter 20.8).

Memory cache size

Maximal memory cache size in the main storage. This cache is used especially to accelerate records to the cache on the disk.
If the value is too high the host's performance can be affected negatively (cache size should not exceed 10 per cent of the computing memory).

Max HTTP object size

maximal size of the object that can be stored in cache.
With respect to statistics, the highest number of requests are for small objects (i.e. HTML pages, images, etc.). Big sized objects, such as archives (that are usually downloaded at once), would require too much memory in the cache.

Cache Options

Advanced options where cache behavior can be defined.

- *Continue aborted download* — tick this option to enable automatic download of objects that have been aborted by the user (using the *Stop* button in a browser). Users often abort downloads for slow pages. If any user attempts to open the same page again, the page will be available in the cache and downloads will be much faster.
- *Cache redirect responses* — HTTP responses that contain redirections will be cached.
- *Use server supplied Time-To-Live* — objects will be cached for time specified by the Web server from which they are downloaded. If TTL is not specified by the server, the default TTL will be used (see the *HTTP protocol TTL* item).
  Warning: Some web servers may attempt to bypass the cache by too short/long TTL.
- *Ignore server Cache-Control directive* — *WinRoute* will ignore directives for cache control of Web pages.
  Pages often include a directive that the page will not be saved into the cache. This directive page may be misused for example to bypass the cache. Enable the *Ignore server Cache-Control directive* option to make *WinRoute* accept only *no-store* and *private* directives.
  Note: WinRoute examines HTTP header directives of responses, not Web pages.
- *Always validate file in cache* — with each query *WinRoute* will check the server for updates of objects stored in the cache (regardless of whether the client demands this).

Note: Clients can always require a check for updates from the Web server (regardless of the cache settings). Use a combination of the *Ctrl+F5* keys to do this using either the *Microsoft Internet Explorer* or the *Firefox/Netscape/Mozilla/SeaMonkey* browser. You can set browsers so that they will check for updates automatically whenever a certain page is opened (then you will only refresh the particular page).

URL Specific Settings

The default cache TTL of an object is not necessarily convenient for each page. You may require not to cache an object or shorten its TTL (i.e. for pages that are accessed daily).

Use the *URL specific settings* button to open a dialog where TTL for a particular URL can be defined.

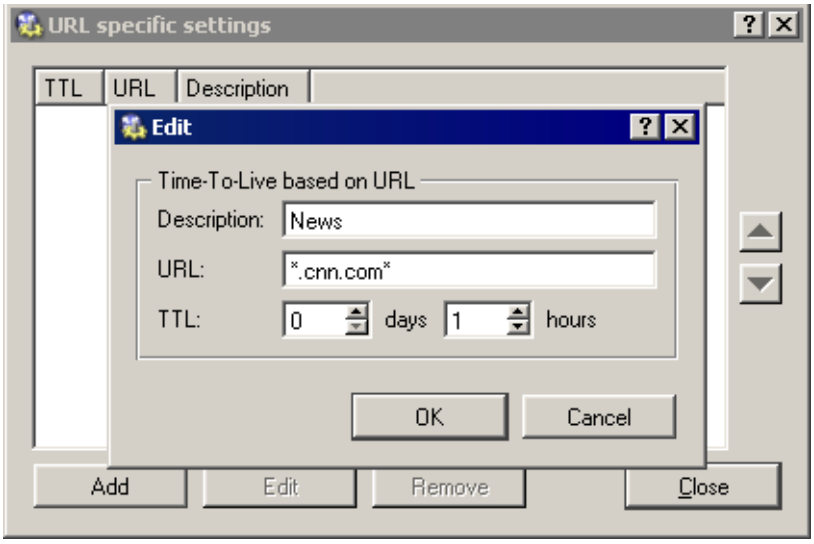


Figure 5.24 HTTP cache — specific settings for URL

Rules within this dialog are ordered in a list where the rules are read one by one from the top downwards (use the arrow buttons on the right side of the window to reorder the rules).

Description

Text comment on the entry (informational purpose only)

URL

URL for which cache TTL will be specified. URLs can have the following forms:

- complete URL (i.e. `www.kerio.com/us/index.html`)
- substring using wildcard matching (i.e. `*news.com*`)
- server name (i.e. `www.kerio.com`) — represents any URL included at the server (the string will be substituted for `www.kerio.com/*` automatically.

TTL

TTL of objects matching with the particular URL.
The *0 days, 0 hours* option means that objects will not be cached.

Cache status and administration

WinRoute allows monitoring of the HTTP cache status as well as manipulation with objects in the cache (viewing and removing).

Note: In older versions of *WinRoute*, these features were included in the web interface whereas since *6.3.0* they are integrated in the *Administration Console*.

At the bottom of the *Cache* tab, basic status information is provided such as the current cache size occupied and efficiency of the cache. The efficiency status stands for number of objects kept in the cache (it is not necessary to download these objects from the server) in proportion to the total number of queries (since the startup of the *WinRoute Firewall Engine*). The efficiency of the cache depends especially on user behavior and habits (if users visit certain webpages regularly, if any websites are accessed by multiple users, etc.) and, in a manner, it can be also affected by the configuration parameters described above. If the efficiency of the cache is permanently low (less than 5 per cent), it is recommended to change the cache configuration.

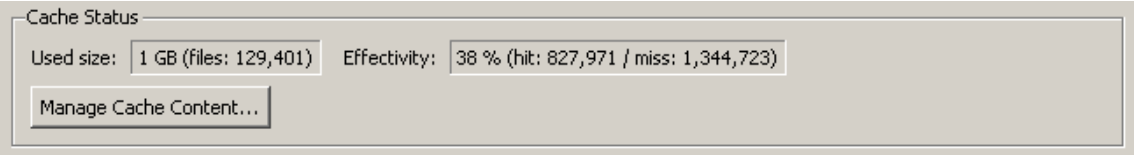


Figure 5.25 HTTP cache status information

Use the *Manage cache content...* button to open a dialog where objects kept in cache can be viewed, searched and/or removed.

To view objects in cache, specify the searched object in the *URL* entry. Objects can be specified either by an absolute URL (without protocol) — e.g. `www.kerio.com/image/menu.gif` or as a URL substring with `*` (substituting any number of any symbols and characters) and `?` (question mark substitutes a single character or symbol) wildcard symbols. Example: Search for the `*ker?o*` string lists all objects with URL matching the specification, such as `kerio`, `kerbo`, etc.

Each line with an object includes URL of the object, its size in bytes (B) and number of hours representing *time left to the expiration*. To keep the list simple and well-organized, up to 100 items are displayed at a single page. The *Previous* and *Next* buttons can be used for browsing through the list pages.

The *Remove* button can be used to delete the selected object from the cache.

TIP: By clicking and dragging or by clicking and using the *Ctrl* or *Shift* key, it is possible to select multiple objects.

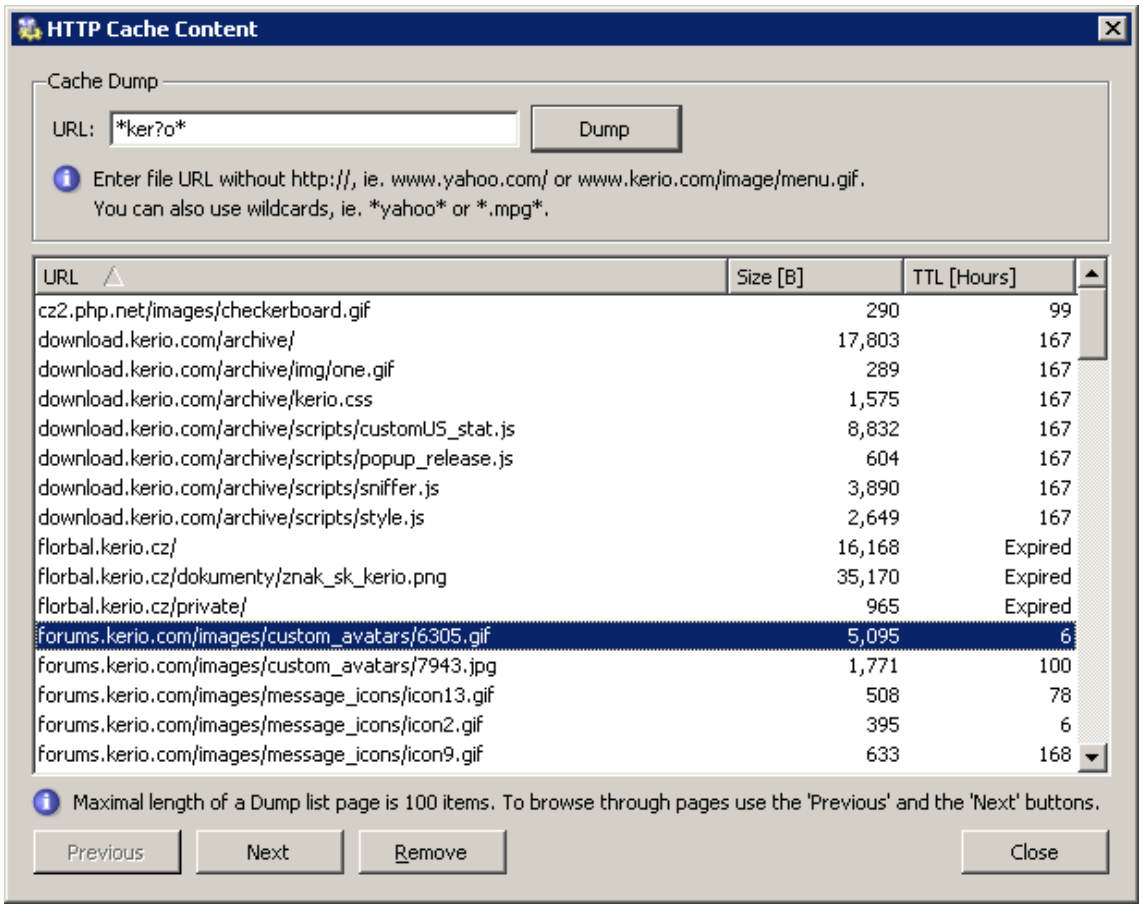


Figure 5.26 HTTP cache administration dialog

Chapter 6

Traffic Policy

Traffic Policy belongs to of the basic *WinRoute* configuration. All the following settings are displayed and can be edited within the table:

- security (protection of the local network including the *WinRoute* host from Internet intrusions
- IP address translation (or NAT, Network Address Translation — technology which enables transparent access of the entire local network to the Internet with one public IP address only)
- access to the servers (services) running within the local network from the Internet (port mapping)
- controlled access to the Internet for local users

Traffic policy rules can be defined in *Configurations* → *Traffic Policy*. The rules can be defined either manually (advanced administrators) or using the wizard (recommended).

It is recommended to create basic traffic rules and later customize them as desired. Advanced administrators can create all the rules according to their specific needs without using the wizard.

6.1 Network Rules Wizard

The network rules wizard demands only the data that is essential for creating a basic set of traffic rules. The rules defined in this wizard will enable access to selected services to the Internet from the local network, and ensure full protection of the local network (including the *WinRoute* host) from intrusion attempts from the Internet. To guarantee reliable *WinRoute* functionality after the wizard is used, all existing rules are removed and substituted by rules created automatically upon the new data.

Click on the *Wizard* button to run the network rules wizard.

Note: The existing traffic policy is substituted by new rules after completing the entire process after confirmation of the last step. This means that during the process the wizard can be stopped and canceled without losing existing rules.

Step 1 — information

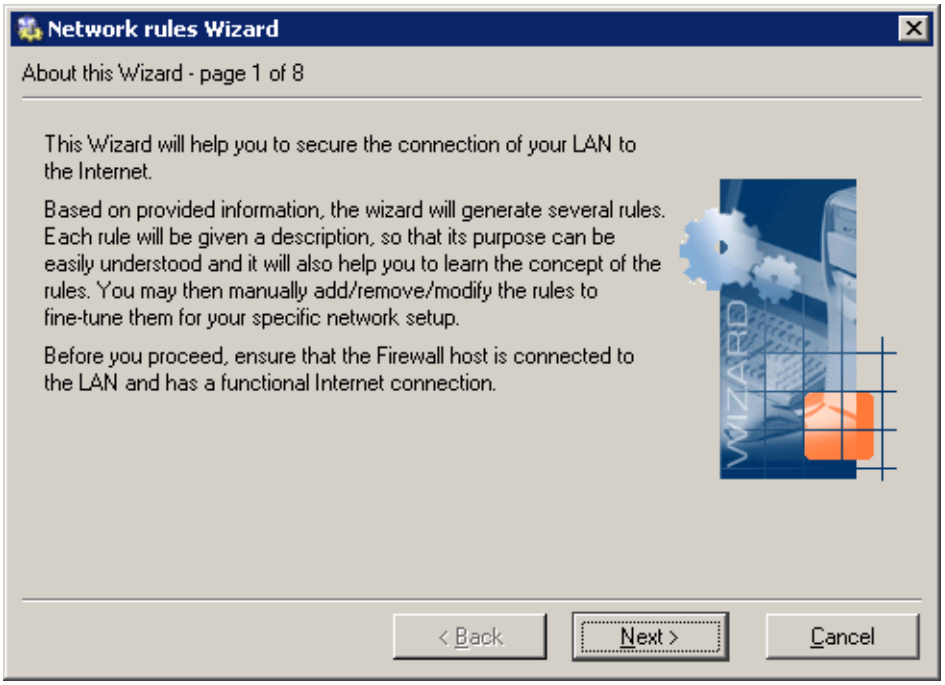

Network rules Wizard
About this Wizard - page 1 of 8
This Wizard will help you to secure the connection of your LAN to the Internet.
Based on provided information, the wizard will generate several rules. Each rule will be given a description, so that its purpose can be easily understood and it will also help you to learn the concept of the rules. You may then manually add/remove/modify the rules to fine-tune them for your specific network setup.
Before you proceed, ensure that the Firewall host is connected to the LAN and has a functional Internet connection.
WIZARD
< Back
Next >
Cancel

Figure 6.1 Traffic Policy Wizard — introduction

To run successfully, the wizard requires the following parameters on the *WinRoute* host:

- at least one active adapter connected to the local network
- at least either one active adapter connected to the Internet or one dial-up defined. The dial-up needn't be active to run the wizard.

Step 2 — selection of Internet connection type

Select the appropriate type of Internet connection that is used — either a network adapter (Ethernet, WiFi, DSL, etc.) or a dialed line (analog modem, ISDN, etc.).

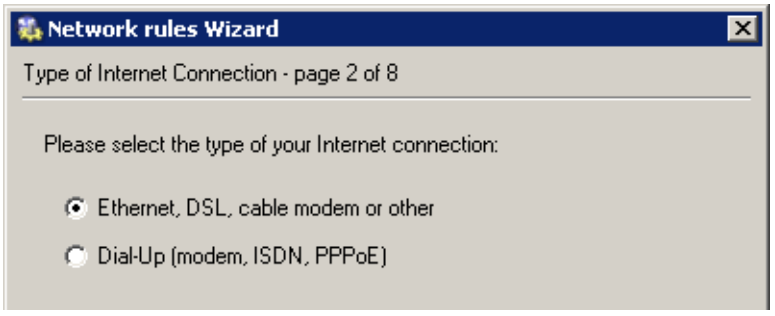

Network rules Wizard
Type of Internet Connection - page 2 of 8
Please select the type of your Internet connection:
Ethernet, DSL, cable modem or other
Dial-Up (modem, ISDN, PPPoE)

Figure 6.2 Network Policy Wizard — selection of Internet connection type

Step 3 — network adapter or dial-up selection

If the network adapter is used to connect the host to the Internet, it can be selected in the menu. To follow the wizard instructions easily, IP address, network mask and MAC address of the selected adapter are displayed as well.

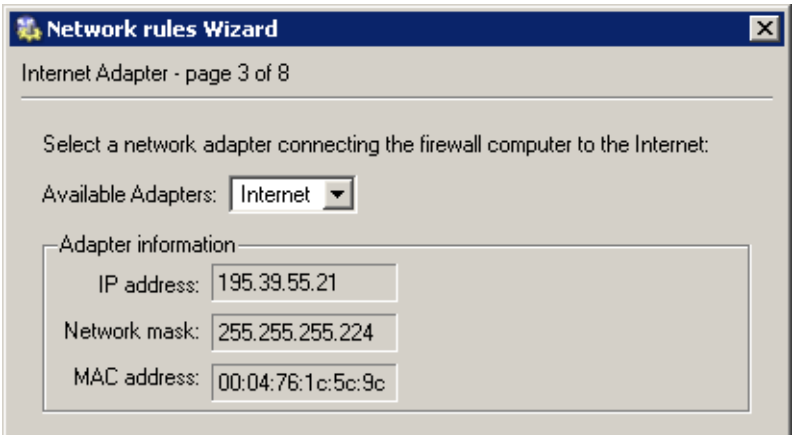


Figure 6.3 Network Policy Wizard — selection of a connected adapter

Note: The Web interface with the default gateway is listed first. Therefore, in most cases the appropriate adapter is already set within this step.

In case of a dial line, the appropriate type of connection (defined in the operating system) must be selected and login data must be specified.

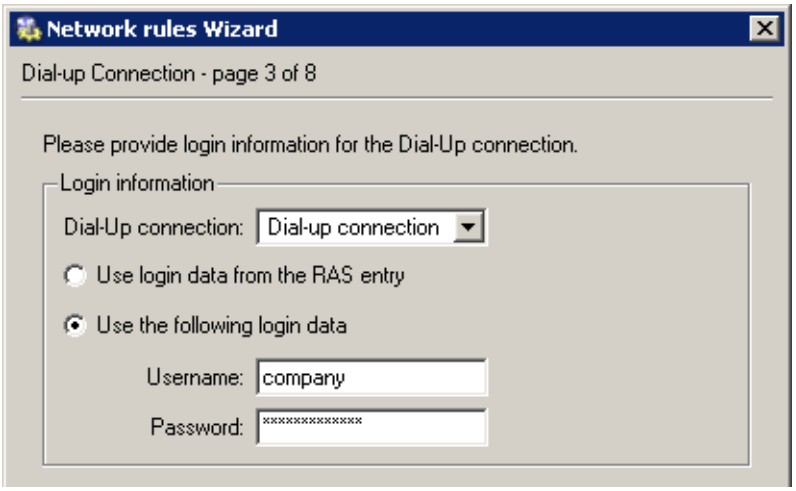


Figure 6.4 Network Policy Wizard — dial-up connection settings

- *Use login data from the RAS entry* — username and password for authentication at the remote server will be copied from a corresponding *Windows* RAS entry. The RAS connection must be saved in the system "phonebook" (the connection must be available to any user).

- *Use the following login data* — specify *Username* and *Password* that will be used for authentication at the remote server. This option can be helpful for example when it is not desirable to save the login data in the operating system or if later it would be edited.

Step 4 — Internet access limitations

Select which Internet services will be available for LAN users:

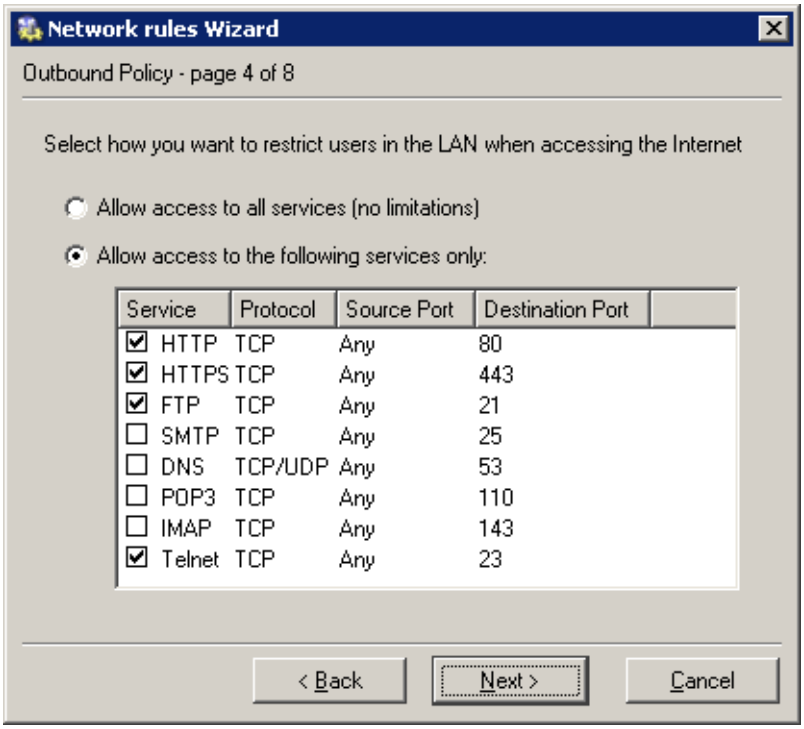

Network rules Wizard
Outbound Policy - page 4 of 8
Select how you want to restrict users in the LAN when accessing the Internet
Allow access to all services (no limitations)
Allow access to the following services only:
Service
Protocol
Source Port
Destination Port
HTTP TCP Any 80
HTTPS TCP Any 443
FTP TCP Any 21
SMTP TCP Any 25
DNS TCP/UDP Any 53
POP3 TCP Any 110
IMAP TCP Any 143
Telnet TCP Any 23
< Back
Next >
Cancel

Figure 6.5 Network Policy Wizard — enabling access to Internet services

Allow access to all services

Internet access from the local network will not be limited. Users can access any Internet service.

Allow access to the following services only

Only selected services will be available from the local network.

Note: In this dialog, only basic services are listed (it does not depend on what services were defined in *WinRoute* — see chapter 12.3). Other services can be allowed by definition of separate traffic policy rules— see chapter 6.3.

Step 5 — enabling Kerio VPN traffic

To use *WinRoute's* proprietary VPN solution in order to connect remote clients or to create tunnels between remote networks, keep the *Create rules for Kerio VPN server* selected. Specific services and address groups for *Kerio VPN* will be added. For detailed information on the proprietary VPN solution, refer to chapter 21.

If you intend not to use the solution or to use a third-party solution (e.g. *Microsoft PPTP*, *Nortel IPSec*, etc.), disable the *Create rules for Kerio VPN* option.

To enable remote access to shared items in the local network via a web browser, keep the *Create rules for Kerio Clientless SSL-VPN* option enabled. This interface is independent from *Kerio VPN* and it can be used along with a third-party VPN solution. For detailed information, see chapter 22.

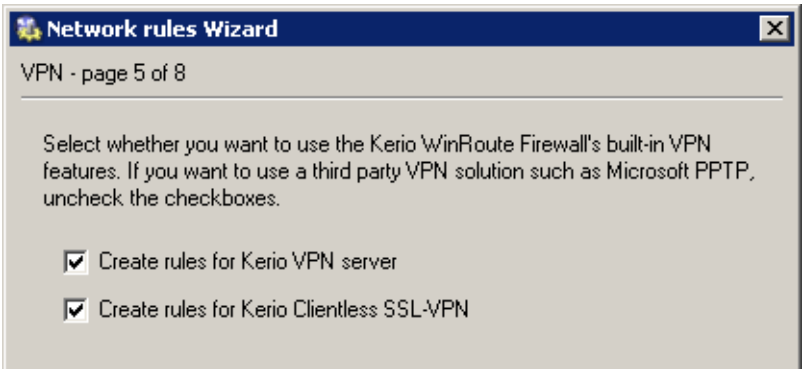

Network rules Wizard
VPN - page 5 of 8
Select whether you want to use the Kerio WinRoute Firewall's built-in VPN features. If you want to use a third party VPN solution such as Microsoft PPTP, uncheck the checkboxes.
Create rules for Kerio VPN server
Create rules for Kerio Clientless SSL-VPN

Figure 6.6 Network Policy Wizard — Kerio VPN

Step 6 — specification of servers that will be available within the local network

If any service (e.g. WWW server, FTP server, etc. which is intended be available from the Internet) is running on the *WinRoute* host or another host within the local network, define it in this dialog.

Note: If creating of rules for Kerio VPN was required in the previous step, the *Kerio VPN* and *HTTPS* firewall services will be automatically added to the list of local servers. If these services are removed or their parameters are modified, VPN services will not be available via the Internet!

The dialog window that will open a new service can be activated with the *Add* button.

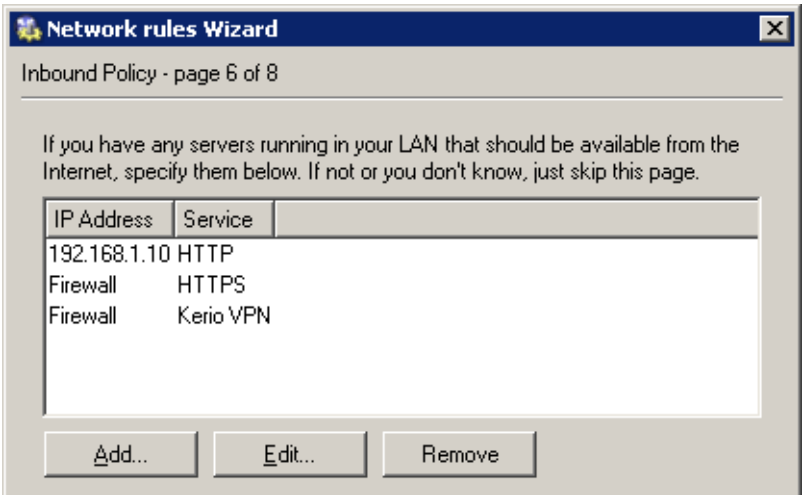

Network rules Wizard
Inbound Policy - page 6 of 8
If you have any servers running in your LAN that should be available from the Internet, specify them below. If not or you don't know, just skip this page.
IP Address
Service
192.168.1.10 HTTP
Firewall HTTPS
Firewall Kerio VPN
Add...
Edit...
Remove

Figure 6.7 Network Policy Wizard — enabling local services

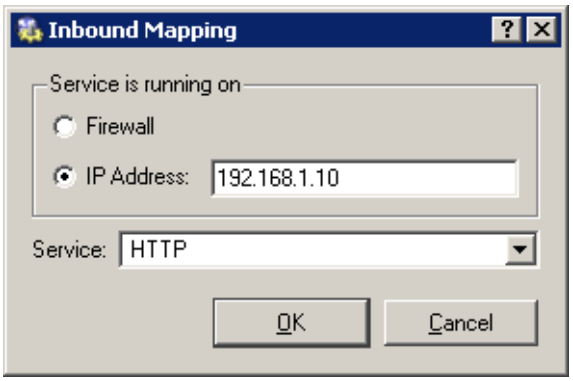


Figure 6.8 Network Policy Wizard — mapping of the local service

Service is running on

Select a computer where the corresponding service is running (i.e. the host to which traffic coming in from the Internet will be redirected):

- *Firewall* — the host where *WinRoute* is installed
- *Local host with IP address* — another host in the local network (local server)
  Note: Access to the Internet through *WinRoute* must be defined at the default gateway of the host, otherwise the service will not be available.

Service

Selection of a service to be enabled. The service must be defined in *Configurations* → *Definitions* → *Services* formerly (see chapter 12.3).
Note: Majority of common services is predefined in *WinRoute*.

Step 7 — NAT

If you only use one public IP address to connect your private local network to the Internet, run the *NAT* function (IP address translation). Do not trigger this function if *WinRoute* is used for routing between two public networks or two local segments (neutral router).

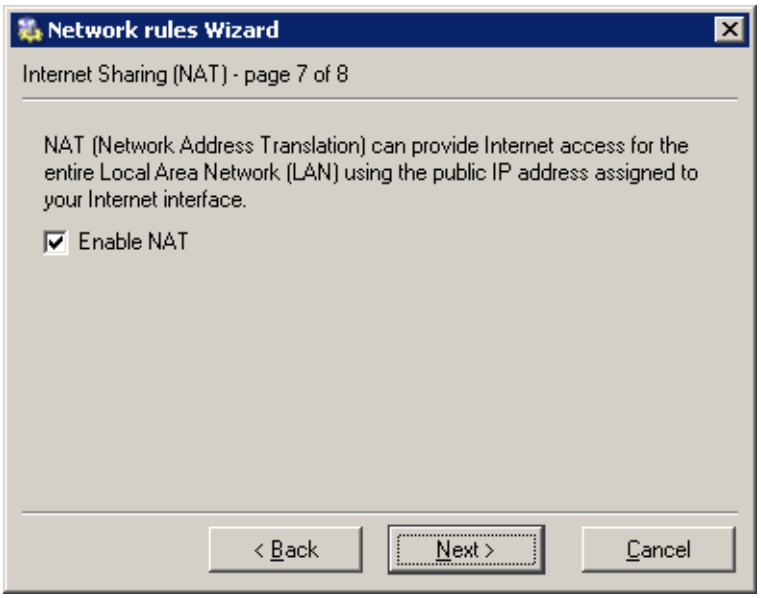

Network rules Wizard
Internet Sharing (NAT) - page 7 of 8
NAT (Network Address Translation) can provide Internet access for the entire Local Area Network (LAN) using the public IP address assigned to your Internet interface.
Enable NAT
< Back
Next >
Cancel

Figure 6.9 Traffic Policy Wizard — Internet connection sharing (NAT)

Step 8 — generating the rules

In the last step, traffic rules are generated in accordance with data specified. All existing rules will be removed and replaced by the new rules.

Warning: This is the last chance to cancel the process and keep the existing traffic policy. Click on the *Finish* button to delete the existing rules and replace them with the new ones.

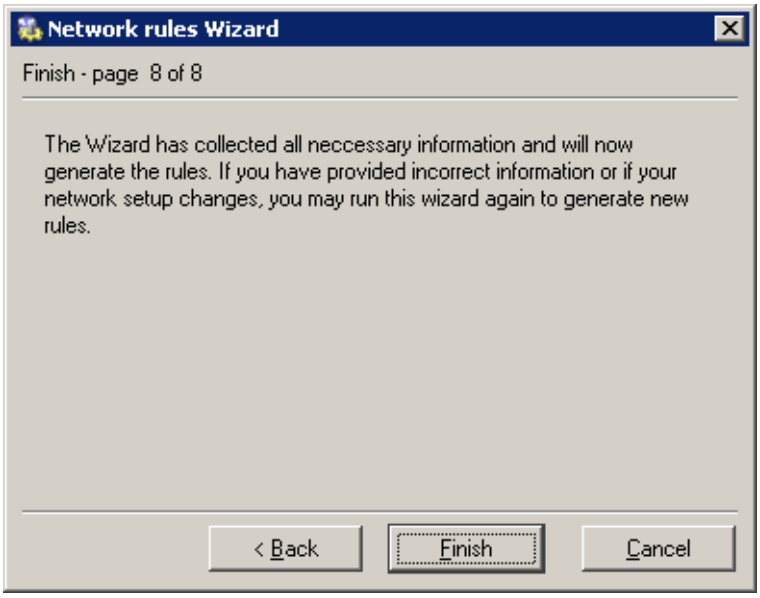

Network rules Wizard
Finish - page 8 of 8
The Wizard has collected all neccessary information and will now generate the rules. If you have provided incorrect information or if your network setup changes, you may run this wizard again to generate new rules.
< Back
Finish
Cancel

Figure 6.10 Network Rules Wizard — the last step

Rules Created by the Wizard

The traffic policy is better understood through the traffic rules created by the Wizard in the previous example.

ICMP traffic

This rule can be added whenever needed with no respect to settings within individual steps. You can use the *PING* command to send a request on a response from the *WinRoute* host. Important issues can be debugged using this command (i.e.Internet connection functionality can be verified).

Note: The *ICMP traffic* rule does not allow clients to use the *PING* command from the local network to the Internet. If you intend to use the command anyway, you must add the *Ping* feature to the *NAT* rules (for details see chapter 6.3).

ISS OrangeWeb Filter

If *ISS OrangeWeb Filter* is used (a module for classification of Websites), this rule is used to allow communication with corresponding databases. Do not disable this traffic, otherwise *ISS OrangeWeb Filter* might not function well.

NAT

If this rule is added, the source (private) addresses in all packets directed from the local network to the Internet will be substituted with addresses of the interface connected to the Internet (see the Wizard, steps 3 and 6). However, only services selected within step 4 can be accessed.

The *Dial-In* interface is included in the *Source* item for this rule. This implies that all *RAS* clients connecting to this server can access the Internet through *NAT*.

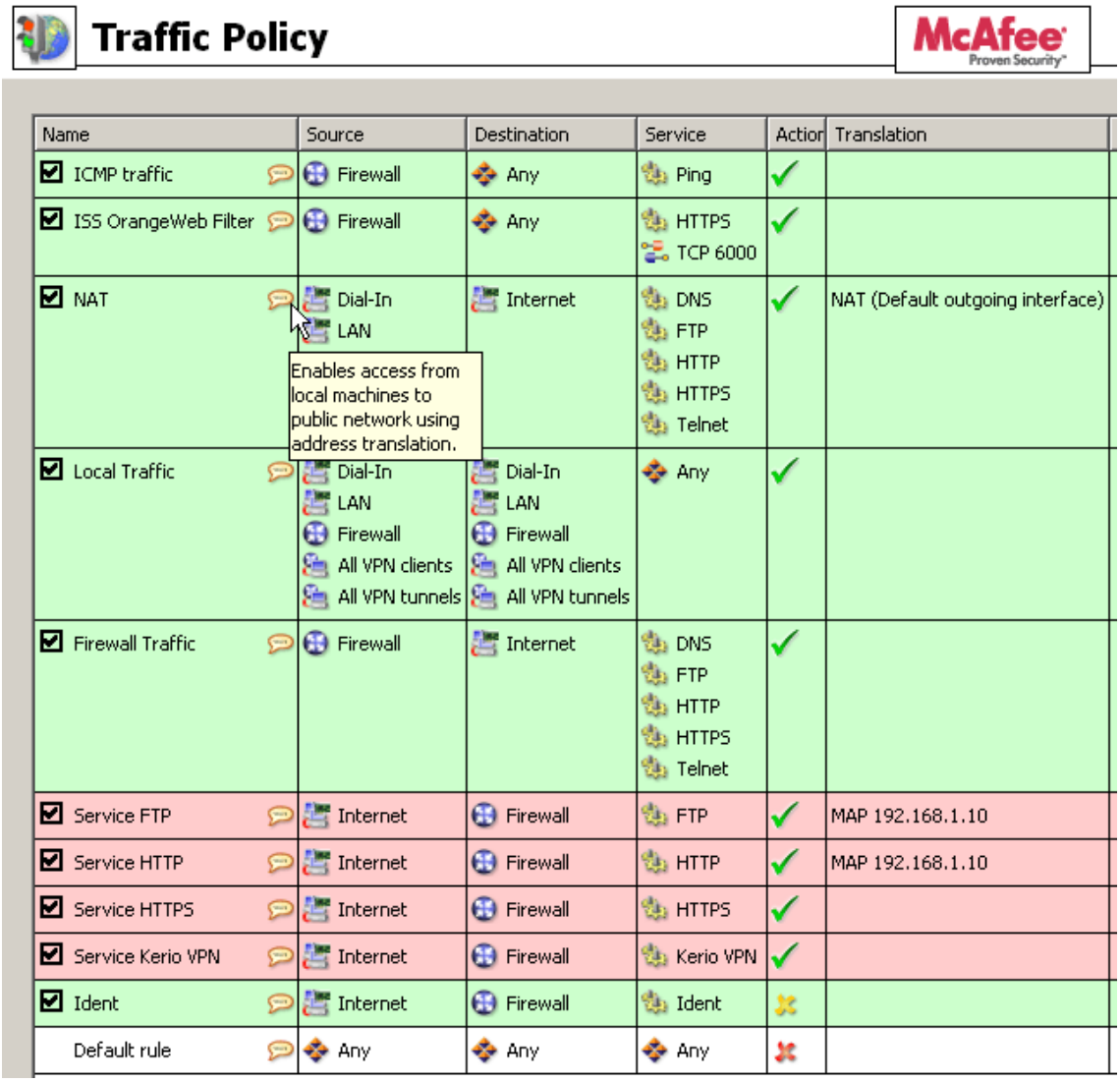


Figure 6.11 Traffic Policy generated by the wizard

Local Traffic

This rule enables all traffic between local hosts and the host where *WinRoute* is installed. The *Source* and *Destination* items within this rule include all *WinRoute* host's interfaces except the interface connected to the Internet (this interface has been chosen in step 3).

In this rule, the *Source* and *Destination* items cover also the *Dial-In* interface and a special group called *Firewall*. This means that the *Local Traffic* rule also allows traffic between local hosts and *RAS* clients/VPN clients connected to the server.

If creating of rules for *Kerio VPN* was set in the wizard (step 5), the *Local Traffic* rule includes also special address groups *All VPN tunnels* and *All VPN clients*.

This implies that, by default, the rule allows traffic between the local network (firewall), remote networks connected via VPN tunnels and VPN clients connecting to the *WinRoute's* VPN server.
Note: Access to the *WinRoute* host is not limited as the Wizard supposes that this host belongs to the local network. Limitations can be done by modification of an appropriate rule or by creating a new one. An inconvenient rule limiting access to the *WinRoute* host might block remote administration or it might cause some Internet services to be unavailable (all traffic directed to the Internet passes through this host).

Firewall Traffic

This rule enables access to certain services from the *WinRoute* host. It is similar to the *NAT* rule except from the fact that this rule does not perform IP translation (this host connects to the Internet directly).

FTP Service and HTTP Service

These rules map all *HTTP* and *HTTPS* services running at the host with the `192.168.1.10` IP address (step 6). These services will be available on IP addresses of the external interface (step 3).

Kerio VPN Service and HTTPS Service

The *Kerio VPN service* rule enables connection to the *WinRoute's* VPN server from the Internet (establishment of control connection between a VPN client and the server or creation of a VPN tunnel — for details, see chapter 21).
The *HTTPS Service* rule allows connection from the Internet via the *Clientless SSL-VPN* interface (access to shared network items via a web browser — for details, see chapter 22).
These rules are not created unless the option allowing access to a particular service is enabled in step 5.

Default rule

This rule denies all communication that is not allowed by other rules. The default rule is always listed at the end of the rule list and it cannot be removed.
The default rule allows the administrator to select what action will be taken with undesirable traffic attempts (*Deny* or *Drop*) and to decide whether packets or/and connections will be logged.

Note: To see detailed descriptions of traffic rules refer to chapter 6.3..

6.2 How traffic rules work

The traffic policy consists of rules ordered by their priority. When the rules are applied they are processed from the top downwards and the first suitable rule found is applied. The order of the rules can be changed with the two arrow buttons on the right side of the window.

An explicit rule denying all traffic is shown at the end of the list. This rule cannot be edited or removed. If there is no rule to allow particular network traffic, then the "catch all" deny rule will discard the packet.

Notes:

1. Unless any other traffic rules are defined (by hand or using the wizard), all traffic is blocked by a special rule which is set as default.

2. To control user connections to WWW or FTP servers, use the special tools available in *WinRoute* (see chapter 10) rather than traffic rules.

6.3 Definition of Custom Traffic Rules

The traffic rules are displayed in the form of a table, where each rule is represented by a row and rule properties (name, conditions, actions — for details see below) are described in the columns. Left-click in a selected field of the table (or right-click a rule and choose the *Edit...* option in the context menu) to open a dialog where the selected item can be edited.

To define new rules press the *Add* button. Move the new rule within the list using the arrow buttons.

Name

Name of the rule. It should be brief and unique. More detailed information can be included in the *Description* entry.

Matching fields next to names can be either ticked to activate or unticked to disable. If a particular field is empty, *WinRoute* will ignore the rule. This means that you need not remove and later redefine these rules when troubleshooting a rule.

The background color of each row can be defined as well. Use the *Transparent* option to make the background transparent (background color of the whole list will be used, white is usually set).

Any text describing the particular rule may be used to specify the *Description* entry (up to 1024 characters).

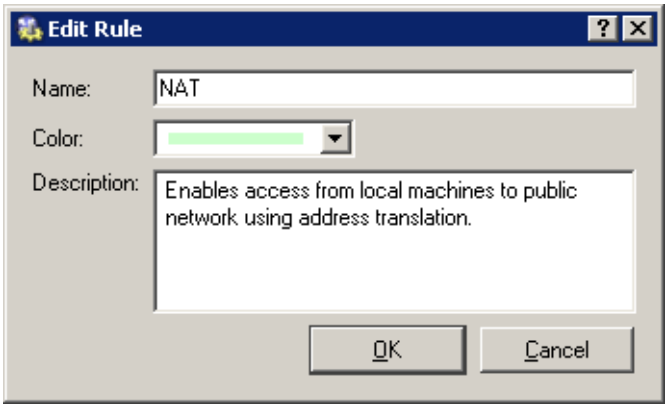


Figure 6.12 Traffic rule — name, color and rule description

If the description is specified, the "bubble" symbol is displayed in the *Name* column next to the rule name. Place the mouse pointer over the bubble to view the rule description.

It is recommended to describe all created rules for better reference (automatic descriptions are provided for rules created by the wizard). This is helpful for later reference (at the first glance, it is clear what the rule is used for). *WinRoute* administrators will appreciate this when fine-tuning or trouble-shooting.

Note: Descriptions and colors do not affect rule functionality.

Source, Destination

Definition of the source or destination of the traffic defined by the rule.

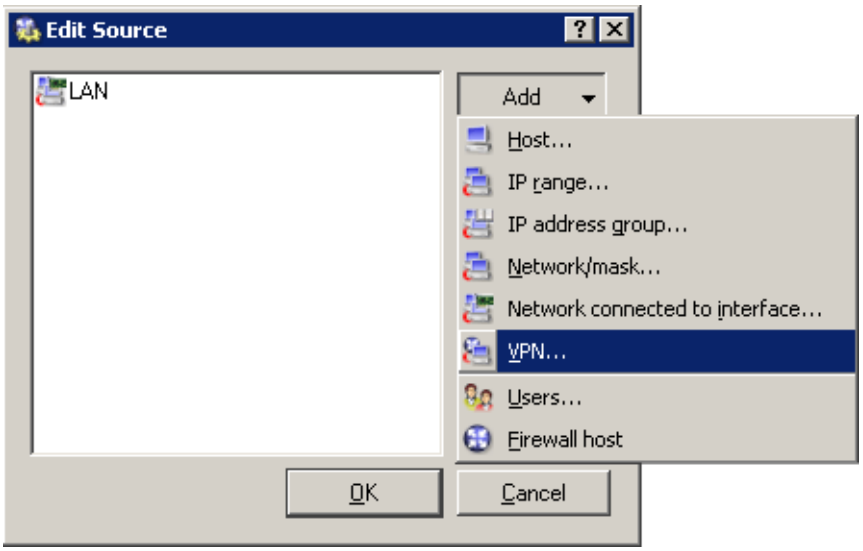


Figure 6.13 Traffic rule — source address definition

A new source or destination item can be defined after clicking the *Add* button:

- *Host* — the host IP address or name (e.g. `192.168.1.1` or `www.company.com`)

  Warning: If either the source or the destination computer is specified by DNS name, *WinRoute* tries to identify its IP address while processing a corresponding traffic rule.

  If no corresponding record is found in the cache, the *DNS forwarder* forwards the query to the Internet. If the connection is realized by a dial-up which is currently hung-up, the query will be sent after the line is dialed. The corresponding rule is disabled unless IP address is resolved from the DNS name. Under certain circumstances denied traffic can be let through while the denial rule is disabled (such connection will be closed immediately when the rule is enabled again).

  For the reasons mentioned above we recommend you to specify source and destination computer only through IP addresses in case that you are connected to the Internet through a dial-up!

- *IP range* — e.g. `192.168.1.10—192.168.1.20`

- *IP address group* — a group of addresses defined in *WinRoute* (refer to chapter 12.1)

- *Subnet with mask* — subnet defined by network address and mask

  (e.g. `192.168.1.0/255.255.255.0`)

- *Network connected to interface* — selection of the interface via which packets come in (*Source*) or via which they are sent (*Destination*)

- *VPN* — virtual private network (created with the *WinRoute* VPN solution). This option can be used to add the following items:

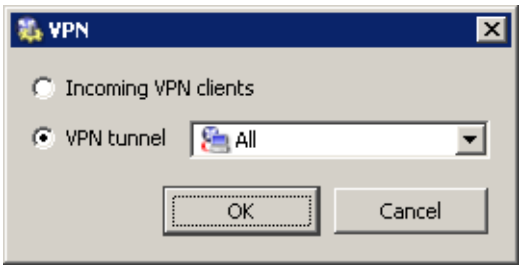


Figure 6.14 Traffic rule — VPN clients / VPN tunnel in the source/destination address definition

1. *Incoming VPN connections (VPN clients)* — all VPN clients connected to the *WinRoute* VPN server via the *Kerio VPN Client*

2. *VPN tunnel* — network connected to this server from a remote server via the VPN tunnel The *All* option covers all networks connected by all VPN tunnels defined which are active at the particular moment.

For detailed information on the proprietary VPN solution integrated in *WinRoute*, refer to chapter 21.

- *Users* — users or groups that can be chosen in a special dialog

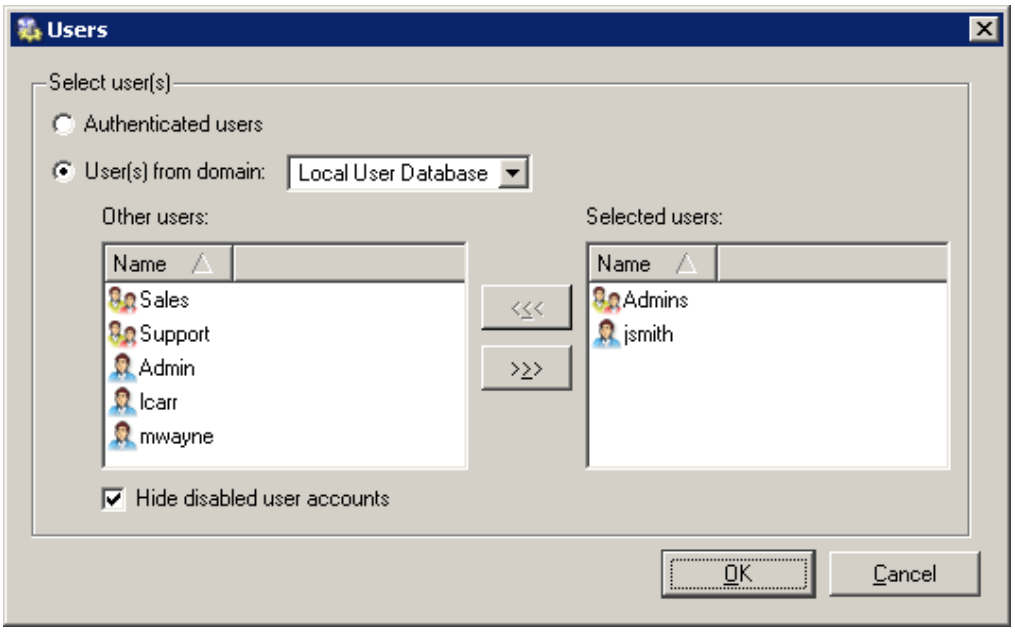


Figure 6.15 Traffic rule — users and groups in the source/destination address definition

The *Authenticated users* option makes the rule valid for all users authenticated to the firewall (see chapter 8.1). Use the *User(s) from domain* option to add users/groups from mapped *Active Directory* domains or from the local user database (for details, refer to chapter 13).

TIP: Users/groups from various domains can be added to a rule at a moment. Select a domain, add users/groups, choose another domain and repeat this process until all demanded users/groups are added.

In traffic rules, user are represented by IP address of the host they are connected (authenticated) from. For detailed description on user authentication, refer to chapter 8.1.

Notes:

1. If you require authentication for any rule, it is necessary to ensure that a rule exists to allow users to connect to the firewall authentication page. If users use each various hosts to connect from, IP addresses of all these hosts must be considered.

2. If user accounts or groups are used as a source in the Internet access rule, automatic redirection to the authentication page nor NTLM authentication will work. Redirection requires successful establishment of connection to the destination server.

   If traffic policy is set like this, users must be told to open the authentication page (see chapters 9 and 8.1) in their browser and login before they are let into the Internet.

   This issue is described in detail in chapter 23.5.

- *Firewall* — a special address group including all interfaces of the host where the firewall is running. This option can be used for example to permit traffic between the local network and the *WinRoute* host.

Use the *Any* button to replace all defined items with the *Any* item (this item is also used by default for all new rules). This item will be removed automatically when at least one new item is added.

Use the *Remove* button to remove all items defined (the *Nothing* value will be displayed in the item list). Whenever at least one item is added, the *Nothing* value will be removed automatically. If the *Nothing* value is kept for the *Source* or/and *Destination* item, a corresponding rule is disabled.

The *Nothing* value takes effect when network interfaces (see chapter 5.1) and users or groups (see chapter 13) are removed . The *Nothing* value is automatically used for all *Source* or/and *Destination* items of rules where a removed interface (or user or a group) has been used. Thus, all these rules are disabled. Inserting the *Nothing* value manually is not meaningful —a checking box in the *Name* column can be used instead.

Note: Removed interfaces cannot be replaced by the *Any* value, otherwise the traffic policy might be changed fundamentally (e.g. an undesirable traffic might be allowed).

Service

Definition of service(s) on which the traffic rule will be applied. Any number of services defined either in *Configurations* → *Definitions* → *Services* (see chapter 12.3) or using protocol and port number (or by port range — a dash is used to specify the range) can be included in the list.

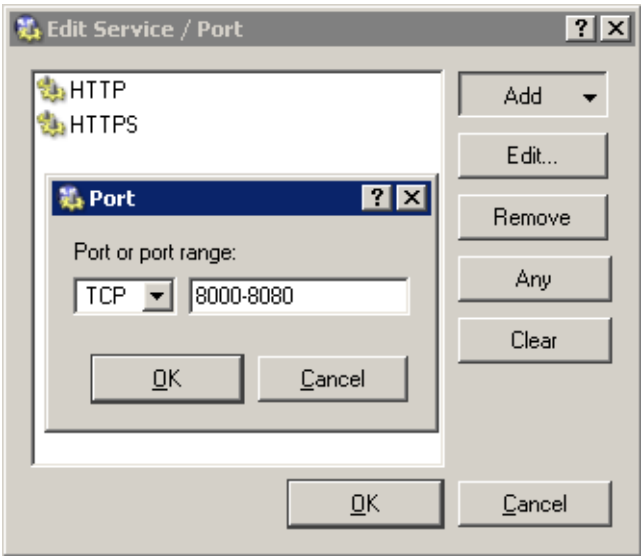


Figure 6.16 Traffic rule — setting a service

Use the *Any* button to replace all defined items with the *Any* item (this item is also used by default for all new rules). Whenever at least one new service is added, the *Any* value removed automatically.

Use the *Remove* button to remove all items defined (the *Nothing* value will be displayed in the item list). Whenever at least one service is added, the *Nothing* value will be removed automatically. If the *Nothing* value is kept in the *Service* column, the rule is disabled.

The *Nothing* value is important for removal of services (see chapter 12.3). The *Nothing* value is automatically used for the *Service* item of rules where a removed service has been used. Thus, all these rules are disabled. Inserting the *Nothing* value manually is not meaningful —a checking box in the *Name* column can be used instead.

Note: If a protocol inspector of the particular protocol is used in the service definition, the inspector is automatically applied to this service's traffic. If desired to bypass the protocol inspector for certain traffic, it is necessary to define this exception in the particular traffic rule. For detailed information, see chapter 23.4.

Action

Action that will be taken by *WinRoute* when a given packet has passed all the conditions for the rule (the conditions are defined by the *Source*, *Destination* and *Service* items). The following actions can be taken:

Figure 6.17 Traffic rule — selecting an action

- *Permit* — traffic will be allowed by the firewall
- *Deny* — client will be informed that access to the address or port is denied. The client will be warned promptly, however, it is informed that the traffic is blocked by firewall.
- *Drop* — all packets that fit this rule will be dropped by firewall. The client will not be sent any notification and will consider the action as a network outage. The action is not repeated immediately by the client (the client expects a response and tries to connect later, etc.).

Note: It is recommended to use the *Deny* option to limit the Internet access for local users and the *Drop* option to block access from the Internet.

Log

The following actions can be taken to log traffic:

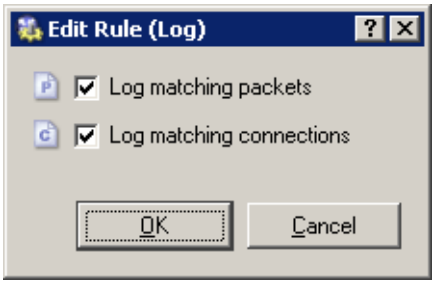


Figure 6.18 Traffic rule — packet/connection logging

- *Log matching packets* — all packets matching with rule (permitted, denied or dropped, according to the rule definition) will be logged in the *Filter* log.
- *Log matching connections* — all connections matching this rule will be logged in the *Connection* log (only for permit rules). Individual packets included in these connections will not be logged.

  Note: Connections cannot be logged for deny nor drop rules.

Translation

Source or/and destination IP address translation.

The source IP address translation can be also called IP masquerading or Internet connection sharing. The source (private) IP address is substituted by the IP address of the interface connected to the Internet in packets routed from the local network to the Internet. Therefore, the entire local network can access the Internet transparently, but it is externally considered as one host.

IP translation is defined as follows:

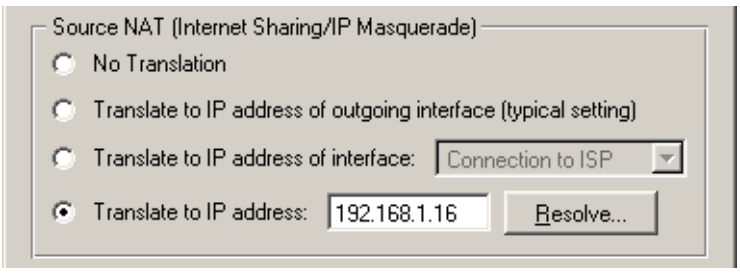


Figure 6.19 Traffic rule — source address translation

- *No Translation* — source address is not modified. This option is set by default and it is not displayed within traffic rules.
- *Translate to IP address of outgoing interface* — *WinRoute* will translate the source address of an outgoing packet to the IP address of the network interface from where the packet will be forwarded.
- *Translate to IP address of interface* — selection of an interface. IP address of the appropriate packet will be translated to the primary address of this interface. This option is relevant if the return path should be different than the upstream path.
- *Translate to IP address* — an IP address to which the source address will be translated (i.e. secondary IP address of an interface connected to the Internet). If you only

know DNS name of your host, use the *Resolve* button to translate the DNS name to IP address.

Warning: The IP address must be assigned to an interface (bound by TCP/IP stack) of the *WinRoute* host!

Destination address translation (also called port mapping) is used to allow access to services hosted behind the firewall. All incoming packets that meet defined rules are re-directed to a defined host (destination address is changed). This actually "moves" to the outbound interface of the *WinRoute* host (i.e. IP address it is mapped from). From the client's point of view, the service is running on the IP address of the Firewall.

Options for destination NAT (port mapping):

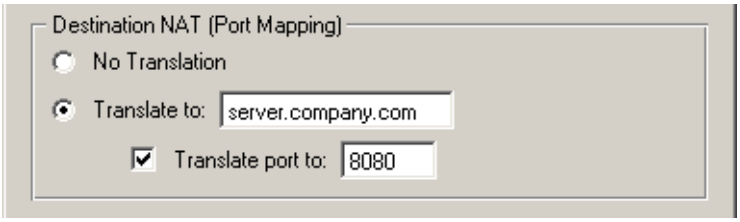


Figure 6.20 Traffic rule — destination address translation

- *No Translation* — destination address will not be modified.
- *Translate to* — IP address that will substitute the packet's destination address. This address also represents the IP address of the host on which the service is actually running.

  The *Translate to* entry can be also specified by DNS name of the destination computer. In such cases *WinRoute* finds a corresponding IP address using a DNS query.

  Warning: We recommend you not to use names of computers which are not recorded in the local DNS since rule is not applied until a corresponding IP address is found. This might cause temporary malfunction of the mapped service.
- *Translate port to* — during the process of IP translation you can also substitute the port of the appropriate service. This means that the service can run at a port that is different from the port from which it is mapped.

  Note: This option cannot be used unless only one service is defined in the *Service* entry within the appropriate traffic rule and this service uses only one port or port range.

The following columns are hidden by the default settings of the *Traffic Policy* dialog:

Valid on

Time interval within which the rule will be valid. Apart from this interval *WinRoute* ignores the rule.

The special *always* option can be used to disable the time limitation (it is not displayed in the *Traffic Policy* dialog).

When a denying rule is applied and/or when an allowing rule's appliance terminates, all active network connections matching the particular rule are closed immediately.

Protocol inspector

Selection of a protocol inspector that will be applied on all traffic meeting the rule. The menu provides the following options to select from:

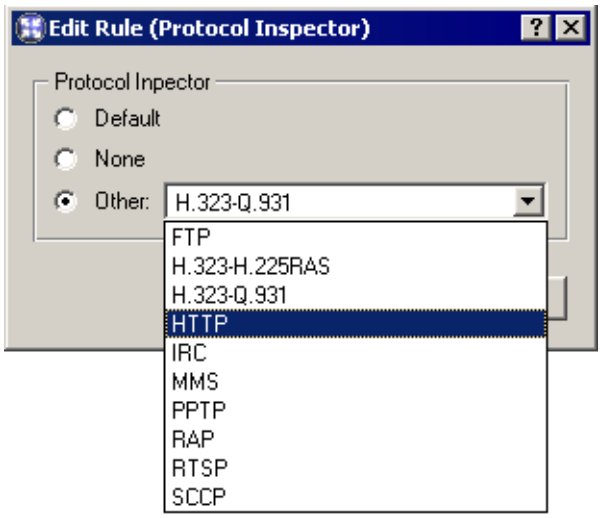


Figure 6.21 Traffic rule — protocol inspector selection

- *Default* — all necessary protocol inspectors (or inspectors of the services listed in the *Service* entry) will be applied on traffic meeting this rule.
- *None* — no inspector will be applied (regardless of how services used in the *Service* item are defined).
- *Other* — selection of a particular inspector which will be used on traffic meeting this rule (all *WinRoute's* protocol inspectors are available).

  Warning: Do not use this option unless the appropriate traffic rule defines a protocol belonging to the inspector. Functionality of the service might be affected by using an inappropriate inspector.

Note: Use the *Default* option for the *Protocol Inspector* item if a particular service (see the *Service* item) is used in the rule definition (the protocol inspector is included in the service definition).

6.4 Basic Traffic Rule Types

WinRoute traffic policy provides a range of network traffic filtering options. In this chapter you will find some rules used to manage standard configurations. Using these examples you can easily create a set of rules for your network configuration.

IP Translation (NAT)

IP translation (as well as Internet connection sharing) is a term used for the exchange of a private IP address in a packet going out from the local network to the Internet with the IP address of the Internet interface of the *WinRoute* host. This technology is used to connect local private networks to the Internet by a single public IP address.

The following example shows an appropriate traffic rule:

Name	Source	Destination	Service	Action	Translation
NAT	LAN	Internet	Any	✓	NAT (Default outgoing interface)

Figure 6.22 A typical traffic rule for NAT (Internet connection sharing)

Source
: Interface connected to the private local network.
If the network includes more than one segment and each segment is connected to an individual interface, specify all the interfaces in the *Source* entry.
If the local network includes other routers, it is not necessary to specify all interfaces (the interface which connects the network with the *WinRoute* host will be satisfactory).

Destination
: Interface connected to the Internet.

Service
: This entry can be used to define global limitations for Internet access. If particular services are defined for IP translations, only these services will be used for the IP translations and other Internet services will not be available from the local network.

Action
: To validate a rule one of the following three actions must be defined: Permit, Drop, Deny.

Translation

In the *Source NAT* section select the *Translate to IP address of outgoing interface* option (the primary IP address of the interface via which packets go out from the *WinRoute* host will be used for NAT).

To use another IP address for the IP translation, use the *Translate to IP address* option and specify the address. The address should belong to the addresses used for the Internet interface, otherwise IP translations will not function correctly.

Warning: The *No translation* option should be set in the *Destination address translation* section, otherwise the rule might not function. Combining source and destination IP address translation is relevant under special conditions only .

Placing the rule

The rule for destination address translation must be preceded by all rules which deny access to the Internet from the local network.

Note: Such a rule allows access to the Internet from any host in the local network, not from the firewall itself (i.e. from the *WinRoute* host)!

Traffic between the firewall and the Internet must be enabled by a special rule. Since *WinRoute* host can access the Internet directly, it is not necessary to use NAT.

Name	Source	Destination	Service	Action	Translation
Firewall traffic	Firewall	Any	Any	✓	

Figure 6.23 Rule for traffic between the firewall and hosts in the Internet

Port mapping

Port mapping allows services hosted on the local network (typically in private networks) to become available over the Internet. The locally hosted server would behave as if it existed directly on the Internet (public address of the *WinRoute* host). The traffic rule therefore must be defined as in the following example:

Name	Source	Destination	Service	Action	Translation
Web server	Internet	Firewall	HTTP HTTPS	✓	MAP 192.168.1.10

Figure 6.24 Traffic rule that makes the local web server available from the Internet

Source

Interface connected to the Internet (requests from the Internet will arrive on this interface).

Destination

The *WinRoute* host labelled as *Firewall*, which represents all IP addresses bound to the firewall host.

This service will be available at all addresses of the interface connected to the Internet. To make the service available at a particular IP address, use the *Host* option and specify the IP address.

Service

Services to be available. You can select one of the predefined services (see chapter 12.3) or define an appropriate service with protocol and port number.

Any service that is intended to be mapped to one host can be defined in this entry. To map services for other hosts you will need to create a new traffic rule.

Action

Select the *Allow* option, otherwise all traffic will be blocked and the function of port mapping will be irrelevant.

Translation

In the *Destination NAT (Port Mapping)* section select the *Translate to IP address* option and specify the IP address of the host within the local network where the service is running.

Using the *Translate port to* option you can map a service to a port which is different from the one where the service is available from the Internet.

Warning: In the *Source NAT* section should be set to the *No Translation* option. Combining source and destination IP address translation is relevant under special conditions only .

Note: For proper functionality of port mapping, the locally hosted server must point to the *WinRoute* firewall as the default gateway. Port mapping will not function well unless this condition is met.

Placing the rule

Port mapping rules are usually independent from NAT rules or/and rules limiting access to the Internet, as well as on each other. For better reference, it is recommended to place all these rules at the top or at the end of the rule list.

If there are special rules limiting access to mapped services, the mapping rules themselves must be placed after the access limiting rules (however, usually it is possible to combine service mapping and access limiting rules and make them a single rule).

Multihoming

Multihoming is a term used for situations when one network interface connected to the Internet uses multiple public IP addresses. Typically, multiple services are available through individual IP addresses (this implies that the services are mutually independent).

Example: In the local network a web server `web1` with IP address `192.168.1.100` and a web server `web2` with IP address `192.168.1.200` are running in the local network. The interface connected to the Internet uses two public IP addresses — `63.157.211.10` and `63.157.211.11`. We want the server `web1` to be available from the Internet at the IP address `63.157.211.10`, the server `web2` at the IP address `63.157.211.11`.

The two following traffic rules must be defined in *WinRoute* to enable this configuration:

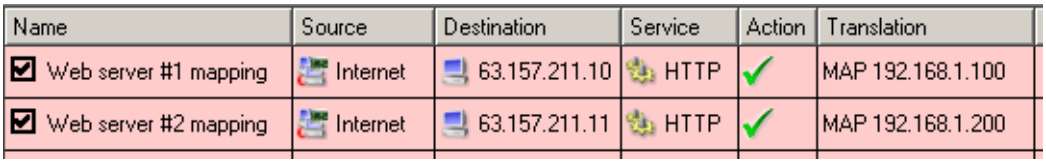


Figure 6.25 Multihoming — web servers mapping

Source
: Interface connected to the Internet (requests from the Internet will arrive on this interface).

Destination
: An appropriate IP address of the interface connected to the Internet (use the *Host* option for insertion of an IP address).

Service
: Service which will be available through this interface (the *HTTP* service in case of a Web server).

Action
: Select the *Allow* option, otherwise all traffic will be blocked and the function of port mapping will be irrelevant.

Translation
: Go to the *Destination NAT (Port Mapping)* section, select the *Translate to IP address* option and specify IP address of a corresponding Web server (`web1` or `web2`).

Limiting Internet Access

Sometimes, it is helpful to limit users access to the Internet services from the local network. Access to Internet services can be limited in several ways. In the following examples, the limitation rules use IP translation. There is no need to define other rules

as all traffic that would not meet these requirements will be blocked by the default "catch all" rule.

Other methods of Internet access limitations can be found in the *Exceptions* section (see below).

Note: Rules mentioned in these examples can be also used if *WinRoute* is intended as a neutral router (no address translation) — in the *Translation* entry there will be no translations defined.

1. Allow access to selected services only. In the translation rule in the *Service* entry specify only those services that are intended to be allowed.

Name	Source	Destination	Service	Action	Translation
NAT	LAN	Internet	DNS FTP HTTP HTTPS Telnet	✓	NAT (Default outgoing interface)

Figure 6.26 Internet connection sharing — only selected services are available

2. Limitations sorted by IP addresses. Access to particular services (or access to any Internet service) will be allowed only from selected hosts. In the *Source* entry define the group of IP addresses from which the Internet will be available. This group must be formerly defined in *Configuration* → *Definitions* → *Address Groups* (see chapter 13.5).

Name	Source	Destination	Service	Action	Translation
NAT for allowed hosts	Internet access	Internet	Any	✓	NAT (Default outgoing interface)

Figure 6.27 Only selected IP address group(s) is/are allowed to connect to the Internet

Note: This type of rule should be used only if each user has his/her own host and the hosts have static IP addresses.

3. Limitations sorted by users. Firewall monitors if the connection is from an authenticated host. In accordance with this fact, the traffic is permitted or denied.

Name	Source	Destination	Service	Action	Translation
NAT for a group of users	[Internet access]	Internet	Any	✓	NAT (Default outgoing interface)

Figure 6.28 Only selected user group(s) is/are allowed to connect to the Internet

Alternatively you can define the rule to allow only authenticated users to access specific services. Any user that has a user account in *WinRoute* will be allowed to access the Internet after authenticating to the firewall. Firewall administrators can easily monitor which services and which pages are opened by each user (it is not possible to connect anonymously).

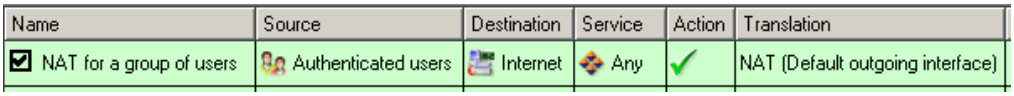


Figure 6.29 Only authenticated users are allowed to connect to the Internet

For detailed description on user authentication, refer to chapter 8.1.

Notes:

1. The rules mentioned above can be combined in various ways (i.e. a user group can be allowed to access certain Internet services only).

2. Usage of user accounts and groups in traffic policy follows specific rules. For detailed description on this topic, refer to chapter 23.5.

Exclusions

You may need to allow access to the Internet only for a certain user/address group, whereas all other users should not be allowed to access this service.

This will be better understood through the following example (how to allow a user group to use the *Telnet* service for access to servers in the Internet). Use the two following rules to meet these requirements:

- First rule will deny selected users (or a group of users/IP addresses, etc.) to access the Internet.

- Second rule will deny the other users to access this service.

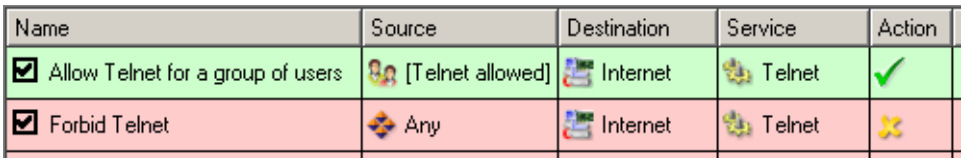


Figure 6.30 Exception — Telnet is available only for selected user group(s)

Chapter 7

Bandwidth Limiter

The main problem of shared Internet connection is when one or more users download or upload big volume of data and occupy great part of the line connected to the Internet (so called bandwidth). The other users are ten limited by slower Internet connection or also may be affected by failures of certain services (e.g. if the maximal response time is exceeded).

The gravest problems arise when the line is overloaded so much that certain network services (such as mailserver, web server or VoIP) must be limited or blocked. This means that, by data downloads or uploads, even a single user may endanger functionality of the entire network.

The *WinRoute's Bandwidth Limiter* module introduces a solution of the most common problems associated with overloads of the Internet connection. This module is capable of recognizing connections where big data volumes are transmitted and it reserves certain part of the line's capacity for these transmissions. The remaining capacity is reserved for the other traffic (where big data volumes are not transmitted but where for example response time may play a role).

7.1 How the bandwidth limiter works and how to use it

The *Bandwidth Limiter* module provides two basic functions:

Speed limits for big data volumes transmissions

WinRoute monitors all connections established between the local network and the Internet. If a connection is considered as a transmission of big data volume, it reduces speed of such transmission to a defined value so that the other traffic is not affected. The bandwidth limiter does not apply to local traffic.
Note: Bandwidth limiting does not depend on traffic rules.

Speed limits for users with their quota exceeded

Users who have exceeded their quota for transmitted amount of data are logically considered as those who are often download or upload big data volumes. *WinRoute* enables to reduce speed of data transmission for these users so that other users and network services are not affected by their network activities. This restriction is automatically applied to users who exceed a quota (see chapter 13.1).

7.2 Bandwidth Limiter configuration

The *Bandwidth Limiter* parameters can be set under *Configuration* → *Bandwidth Limiter*.

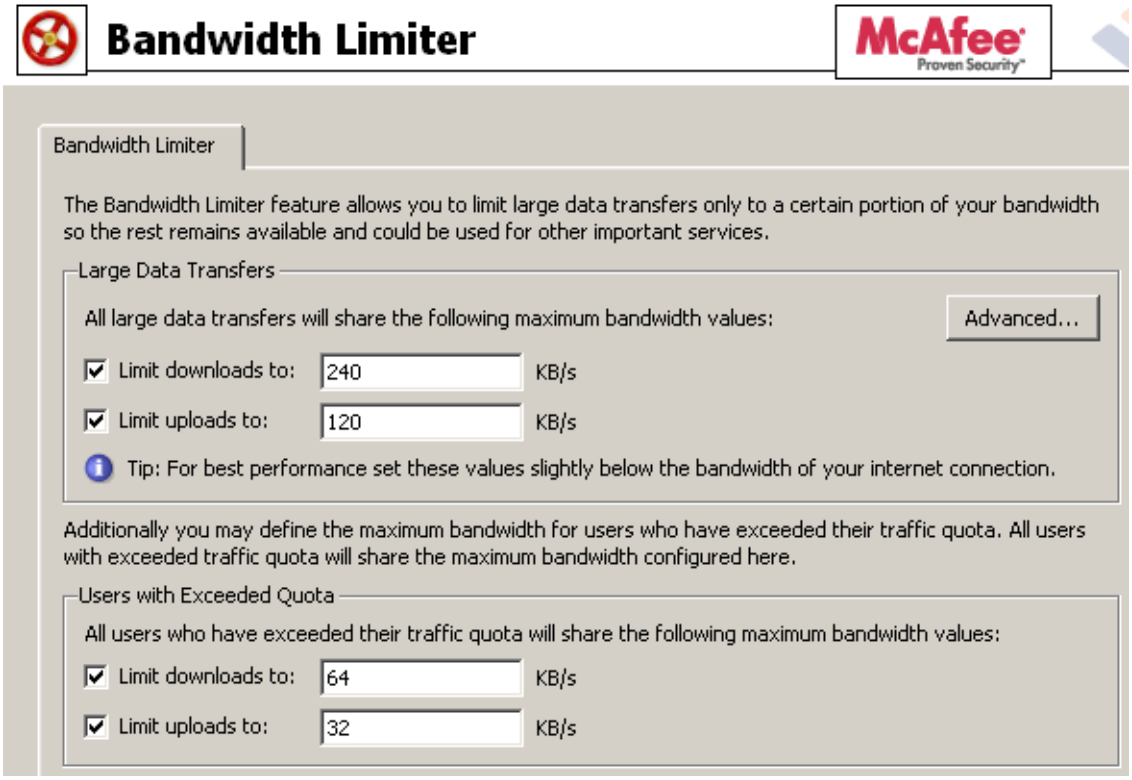

Bandwidth Limiter
McAfee
Proven Security
Bandwidth Limiter
The Bandwidth Limiter feature allows you to limit large data transfers only to a certain portion of your bandwidth so the rest remains available and could be used for other important services.
Large Data Transfers
All large data transfers will share the following maximum bandwidth values:
Advanced...
Limit downloads to: 240 KB/s
Limit uploads to: 120 KB/s
Tip: For best performance set these values slightly below the bandwidth of your internet connection.
Additionally you may define the maximum bandwidth for users who have exceeded their traffic quota. All users with exceeded traffic quota will share the maximum bandwidth configured here.
Users with Exceeded Quota
All users who have exceeded their traffic quota will share the following maximum bandwidth values:
Limit downloads to: 64 KB/s
Limit uploads to: 32 KB/s

Figure 7.1 Bandwidth Limiter configuration

The *Bandwidth Limiter* module enables to define reduction of speed of incoming traffic (i.e. from the Internet to the local network) and of outgoing data (i.e. from the local network to the Internet) for transmissions of big data volumes and for users with their quota exceeded. These limits do not depend on each other. This means it is possible to use one of these functions, both or none.

Warning: In the *Bandwidth Limiter* module, speed is measured in kilobytes per second (*KB/s*). while ISPs usually use kilobits per second (*kbps*, *kbit/s* or *kb/s*), or in megabits per second (*Mbps*, *Mbit/s* or *Mb/s*). The conversion pattern is *1 KB/s = 8 kbit/s*. Example: A *256 kbit/s* line's speed is *32 KB/s*, a *1 Mbit/s* line's speed is *128 KB/s*.

Setting limit values

The top of the dialog box contains a section where limits for transfers of big data volumes can be set. These values determine bandwidth that will be reserved for these transfers. The remaining bandwidth is available for other traffic.

Tests have discovered that the optimal usage of the Internet line capacity is reached if the value is set to approximately 90 per cent of the bandwidth. It the values are higher, the bandwidth limiter is not effective (not enough speed is reserved for other connections and services if too much big data volumes are transferred). If they are lower, full line capacity is often not employed.

Warning: For optimal configuration, it is necessary to operate with *real* capacity of the line. This value may differ from the information provided by ISP. One method of how to find out the real value of the line capacity is to monitor traffic charts (see chapter 18.1) when you can be almost sure that the line is fully employed.

At the bottom of the dialog box, download and upload speed limits for users with exceeded traffic quota can be set. The bandwidth defined will be shared by all users with their quota exceeded. This implies that the total traffic volume of these users is limited by the bandwidth value set here.

No optimal values are known for these speed limits. *WinRoute* administrators decide themselves what part of the bandwidth will be reserved for these users. It is recommended to set the values so that activities of these users do not affect other users and services.

Note: It is also possible to block any traffic for a particular users who exceed their quota. The restriction described above are applied only if the *Don't block further traffic (Only limit bandwidth...)* action is set in configuration of the particular user account. For details, see chapter 13.1.

Advanced Options

Click on *Advanced* to define advanced *Bandwidth Limiter* parameters. These parameters apply only to large data volume transfers. They do not apply to users with exceeded quota (bandwidth values set for these users are applied without exception).

Services

Certain services may seem to perform large data volume transfers, although, in fact, they don't. Internet telephony (*Voice over IP — VoIP*) is a typical example. It is possible to define exceptions for such services so that the bandwidth limiter does not apply to them.

It may also be desired to apply bandwidth limiter only to certain network services (e.g. when it is helpful to limit transfers via *FTP* and *HTTP*).

The *Services* tab enables definition of services to which bandwidth limiter will be applied:

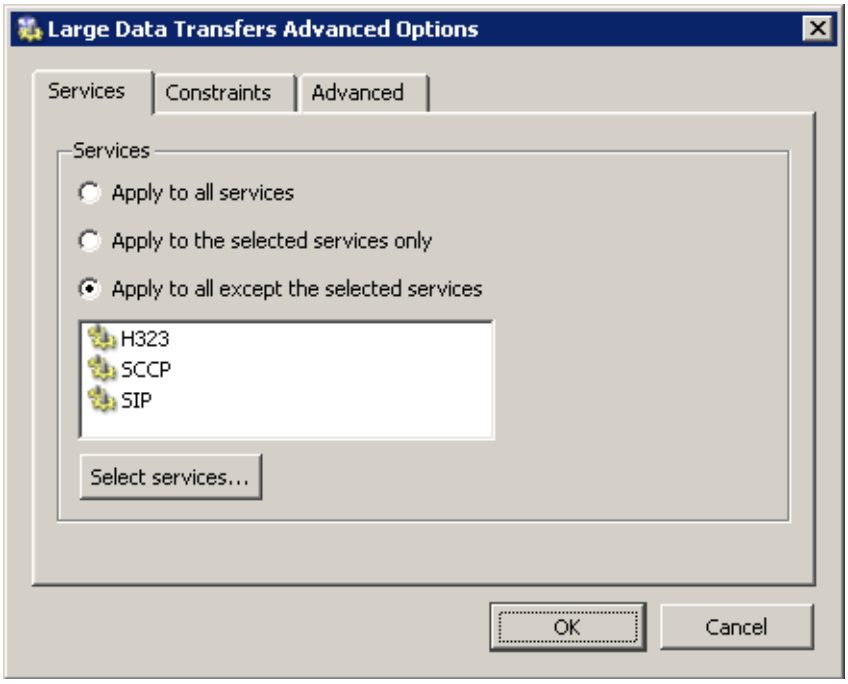


Figure 7.2 Bandwidth Limiter — network services

- *Apply to all services* — the limits will be applied to all traffic between the local network and the Internet.
- *Apply to the selected services only* — the limits will apply only to the selected network services. Traffic performed by other services is not limited.
- *Apply to all except the selected services* — services specified in this section will be excluded from the bandwidth limiter restrictions, whereas the limiter will apply to any other services.

Click on *Select services* to open a dialog box where network services can be selected. Hold the *Ctrl* or the *Shift* key to select multiple services. All services defined in *Configuration* → *Definitions* → *Services* are available (for details, refer to chapter sect-services"/>).

IP Addresses and Time Interval

It may be also helpful to apply bandwidth limiter only to certain hosts (for example, it may be undesired to limit a mailserver in the local network or communication with the corporate web server located in the Internet). This exclusive IP group may contain any IP addresses across the local network and the Internet. Where user workstations use fixed IP addresses, it is also possible to apply this function to individual users.

It is also possible to apply bandwidth limiter to a particular time interval (e.g. in work hours).

These parameters can be set on the *Constraints* tab.

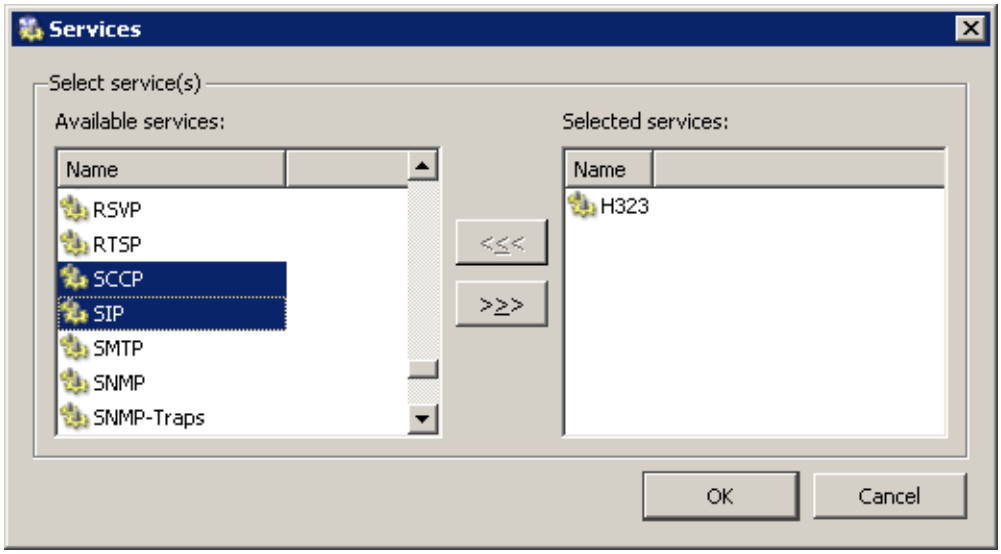


Figure 7.3 Bandwidth Limiter — selection of network services

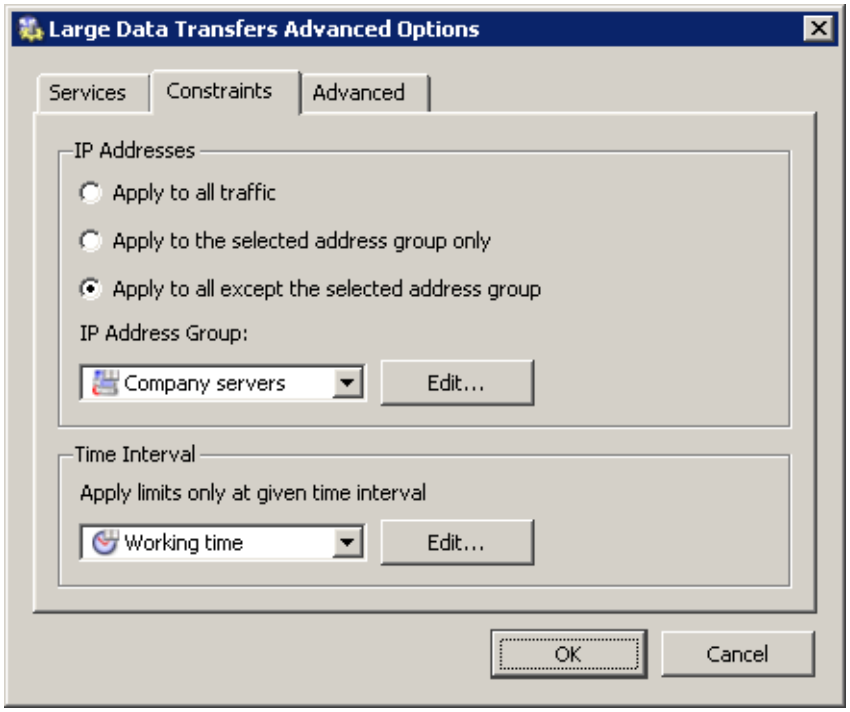


Figure 7.4 Bandwidth Limiter — IP Addresses and Time Interval

At the top of the *Constraints* tab, select a method how bandwidth will be applied to IP addresses and define the IP address group:

- *Apply to all traffic* — the IP address group specification is inactive it is irrelevant.
- *Apply to the selected address group only* — the bandwidth limiter will be applied only if at least one IP address involved in a connection belongs to the address

group. The other traffic will not be limited.

- *Apply to all except the selected address group* — the bandwidth limiter will not be applied if at least one IP address involved in a connection belongs to the address group. Any other traffic will be limited.

In the lower section of the *Constraints* tab, a time range within which the bandwidth would be limited can be set. Click *Edit* to edit the selected interval or to create a new one (details in chapter 12.2).

Setting of parameters for detection of large data volume transfers

The *Advanced* tab enables setting of parameters that will be used for detection of transmissions of large data volume — the minimal volume of transmitted data and inactivity time interval. The default values (*200 KB* and *5 sec*) are optimized in accordance with long-term testing in full action.

Caution! Changes of these values may reduce Bandwidth Limiter performance dramatically. With exception of special conditions (testing purposes) it is highly recommended not to change the default values!

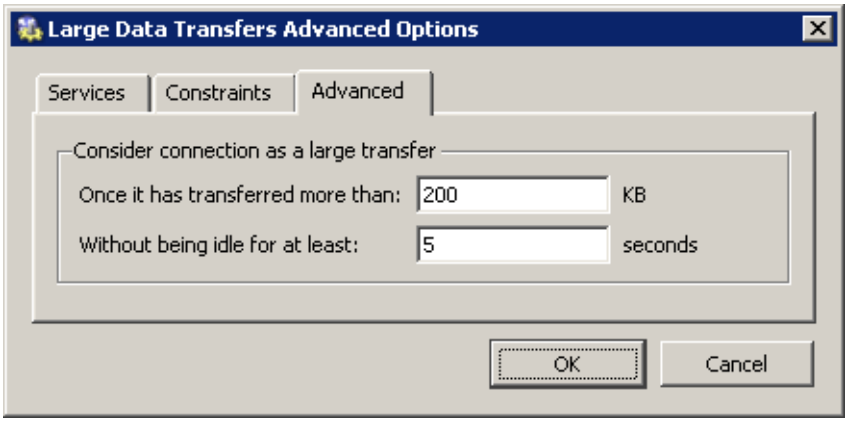


Figure 7.5 Bandwidth Limiter — setting parameters for detection of large data volume transfers

For detailed description of the detection of large data volume transmissions, refer to chapter 7.3.

7.3 Detection of connections with large data volume transferred

This chapter provides description of the method used by the *Bandwidth Limiter* module to detect connections where large data volumes are transmitted. This description is an extra information which is not necessary for usage of the *Bandwidth Limiter* module.

Network traffic is different for individual services. For example, web browsers usually access sites by opening one or more connections and using them to transfer certain amount of data (objects included at the page) and then closes the connections. Terminal services (e.g. *Telnet*, *SSH*, etc.) typically use an open connection to transfer small

data volumes in longer intervals. Large data volume transfers typically uses the method where the data flow continuously with minimal intervals between the transfer impulses.

Two basic parameters are tested in each connection: volume of transferred data and duration of the longest idle interval. If the specified data volume is reached without the idleness interval having been tresholded, the connection is considered as a transfer of large data volume and corresponding limits are applied.

If the idle time exceeds the defined value, the transferred data counter is set to zero and the process starts anew. This implies that each connection that *once* reaches the defined values is considered as a large data volume transfer.

The value of the limit for the amount of data transmitted and the minimal idleness period are configuration parameters of the *Bandwidth Limiter* (see chapter 7.2).

Examples:

The detection of connections transferring large data volumes will be better understood through the following examples. The default configuration of the detection is as follows: at least *200 KB* of data must be transferred while there is no interruption for *5 sec* or more.

1. The connection at figure 7.6 is considered as a transmission of large data volume after transfer of the third load of data. At this point, the connection has transferred 200 KB of data while the longest idleness interval has been only 3 sec.

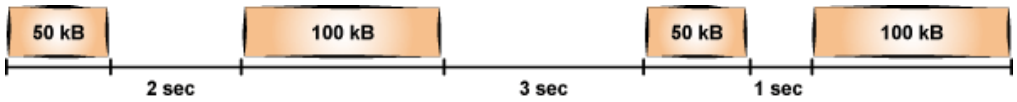


Figure 7.6 Connection example — short idleness intervals

2. Connection at figure 7.7 is not considered as a large data volume transfer, since after 150 KB of data have been transferred before an only 5 sec long idleness interval and then, only other 150 KB of data have been transmitted within the connection.

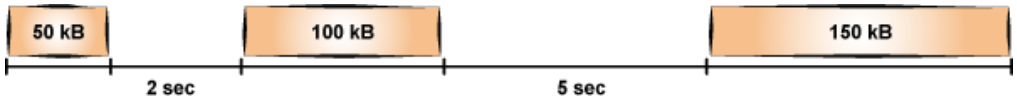


Figure 7.7 Connection example — long idleness interval

3. The connection shown at figure 7.8 transfers 100 KB of data before a 6 sec idleness interval. For this reason, the counter of transferred data is set to zero. Other three blocks of data of 100 KB are then transmitted. When the third block of data is transferred, only 200 KB of transmitted data are recorded at the counter (since the last long idleness interval). Since there is only a 3 sec idleness interval between transmission of the second and the third block of data, the connection is considered as a large data volume transfer.

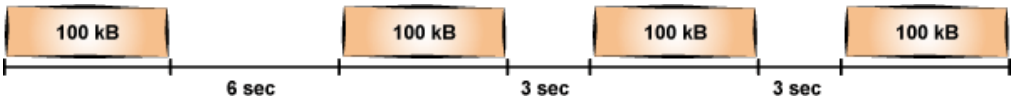


Figure 7.8 Connection example — long idleness interval at the beginning of the transfer

Chapter 8

User Authentication

WinRoute allows administrators to monitor connections (packet, connection, Web pages or FTP objects and command filtering) related to each user. The username in each filtering rule represents the IP address of the host(s) from which the user is connected (i.e. all hosts the user is currently connected from). This implies that a user group represents all IP addresses its members are currently connected from.

In addition to authentication based access limitations, user login can be used to effectively monitor activity using logs (see chapter 2020)), and status (see chapter 17.2) and hosts and users (see chapter 17.1). If there is no user connected from a certain host, only the IP address of the host will be displayed in the logs and statistics.

8.1 Firewall User Authentication

Any user with their own account in *WinRoute* can authenticate at the firewall (regardless their access rights). Users can connect:

- Manually — by opening the *WinRoute* web interface in their browser

  `https://server:4081/` or `http://server:4080/`

  (the name of the server and the port numbers are examples only — see chapter 9).

  It is also possible to authenticate for viewing of the web statistics (see chapter 19) at

  `https://server:4081/star` or `http://server:4080/star`

  The user will be also authenticated at the firewall within this authentication.

- Redirection — when accessing any website (unless access to this page is explicitly allowed to unauthenticated users — see chapter 10.2).

- Using NTLM — if *Microsoft Internet Explorer* or *Firefox/Netscape/Mozilla/SeaMonkey* is used and the user is authenticated in a Windows NT domain or Active Directory, the user can be authenticated automatically (the login page will not be displayed). For details, see chapter 23.3.

- Automatically — IP addresses of hosts from which they will be authenticated automatically can be associated with individual users. This actually means that whenever

traffic coming from the particular host is detected, *WinRoute* assumes that it is currently used by the particular user , and the user is considered being authenticated from the IP address. However, users may authenticate from other hosts (using the methods described above).

IP addresses for automatic authentication can be set during definition of user account (see chapter 13.1).

Note: This authentication method is not recommended for cases where hosts are used by multiple users (user's identity might be misused easily).

Login by re-direction is performed in the following way: user enters URL pages that he/she intends to open in the browser. *WinRoute* detects whether the user has already authenticated. If not, *WinRoute* will re-direct the user to the login page automatically. After a successful login, the user is automatically re-directed to the requested page or to the page including the information where the access was denied.

Note: Users will be redirected to a secured or unsecured web interface according to the fact which version of web interface is allowed (see chapter 9.1). If both versions are allowed, the secured web interface will be used.

User authentication advanced options

Login/logout parameters can be set on the *Authentication Options* tab under *Users and Groups* → *Users*.

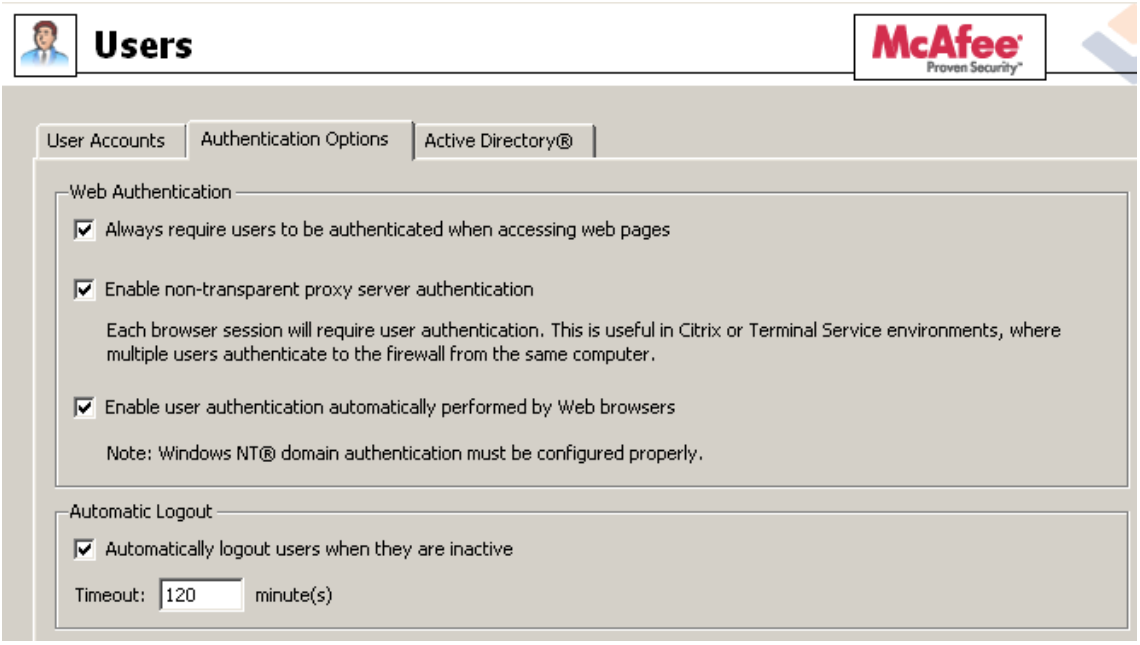

Users
McAfee
Proven Security
User Accounts
Authentication Options
Active Directory®
Web Authentication
Always require users to be authenticated when accessing web pages
Enable non-transparent proxy server authentication
Each browser session will require user authentication. This is useful in Citrix or Terminal Service environments, where multiple users authenticate to the firewall from the same computer.
Enable user authentication automatically performed by Web browsers
Note: Windows NT® domain authentication must be configured properly.
Automatic Logout
Automatically logout users when they are inactive
Timeout:
120
minute(s)

Figure 8.1 User Authentication Options

Redirection to the authentication page

If the *Always require users to be authenticated when accessing web pages* option is enabled, user authentication will be required for access to any website (unless the user is already authenticated). The method of the authentication request depends on the method used by the particular browser to connect to the Internet:

- *Direct access* — the browser will be automatically redirected to the authentication page of the *WinRoute's* web interface (see chapter 9.2) and, if the authentication is successful, to the solicited web page.
- *WinRoute proxy server* — the browser displays the authentication dialog and then, if the authentication is successful, it opens the solicited web page.

If the *Always require users to be authenticated when accessing web pages* option is disabled, user authentication will be required only for Web pages which are not available (are denied by URL rules) to unauthenticated users (refer to chapter 10.2).
Note: User authentication is used both for accessing a Web page (or/and other services) and for monitoring of activities of individual users (the Internet is not anonymous).

Enable non-transparent proxy server authentication

Under usual circumstances, a user connected to the firewall from a particular computer is considered as authenticated by the IP address of the host until the moment when they log out manually or are logged out automatically for inactivity. However, if the client station allows multiple users connected to the computer at a moment (i.e. *Microsoft Terminal Services*, *Citrix Presentation Server* or*Fast user switching* on *Windows XP*), the firewall requires authentication only from the user who starts to work on the host as the first. The other users will be authenticated as this user.
In case of *HTTP* and *HTTPS*, this technical obstruction can be passed by. In web browsers of all clients of the multi-user system, set connection to the Internet via the *WinRoute's* proxy server (for details, see chapter 5.5), and enable the *Enable non-transparent proxy server* option in *WinRoute*. The proxy server will require authentication for each new session of the particular browser.[3].

Automatic authentication (NTLM)

If the *Enable user authentication automatically..* option is checked and *Microsoft Internet Explorer* (version 5.01 or later) or *Firefox/Netscape/Mozilla/SeaMonkey* (core version 1.3 or later) is used, it is possible to authenticate the user automatically using the NTLM method.
This means that the browser does not require username and password and simply uses the identity of the first user connected to *Windows*. However, the NTLM

[3] *Session* is every single period during which a browser is running. For example, in case of *Internet Explorer*, *Firefox* and *Opera*, a session is terminated whenever all windows and tabs of the browser are closed, while in case of *Netscape/Mozilla/SeaMonkey*, a session is not closed unless the *Quick Launch* program is stopped (an icon is displayed in the toolbar's notification area when the program is running).

method is not available for other operating systems.
For details, refer to chapter 23.3.

Automatically logout users when they are inactive

Timeout is a time interval (in minutes) of allowed user inactivity. When this period expires, the user is automatically logged out from the firewall. The default timeout value is 120 minutes (2 hours).
This situation often comes up when a user forgets to logout from the firewall. Therefore, it is not recommended to disable this option, otherwise login data of a user who forgot to logout might be misused by an unauthorized user.

Chapter 9

Web Interface

WinRoute contains a special Web server that can be used for several purposes, such as an interface for user authentication and setting of certain user account parameters. This Web server is available over SSL or using standard HTTP with no encryption (both versions include identical pages).

Use the following URL (`'server'` refers to the name or IP of the *WinRoute* host, `4080` represents a standard HTTP interface port) to open the unsecured version of the web interface.

```
https://server:4081/
```

To use the encrypted version specify the HTTPS protocol and number of the port of the encrypted Web interface (default is `4081`) — e.g.

```
https://server:4081/
```

Note: This chapter addresses settings of web interface parameters and user preferences (available to all users). Statistics viewed in the web interface (available only to users possessing appropriate rights) are addressed in chapter 19.

9.1 Web Interface Parameters Configuration

To define basic *WinRoute* Web interface parameters go to the *Web Interface* folder in *Configuration* → *Advanced Options*.

Note: The top part of the *Web Interface* → *SSL-VPN* tab is used for *Kerio SSL-VPN* settings. For detailed information on this component, see chapter 22.

Enable Kerio SSL-VPN server

This option enables/disables the *Kerio Clientless SSL-VPN* interface. For details, refer to chapter 22.

Enable Web Interface (HTTP)

Use this option to open the unsecured version (HTTP) of the Web interface The default port for this unsecured interface is `4080`.

Note: The main disadvantage of usage of the unsecured web interface is that the network traffic may be tapped and user login data might be misused. Therefore, the secured web interface shall be always preferred.

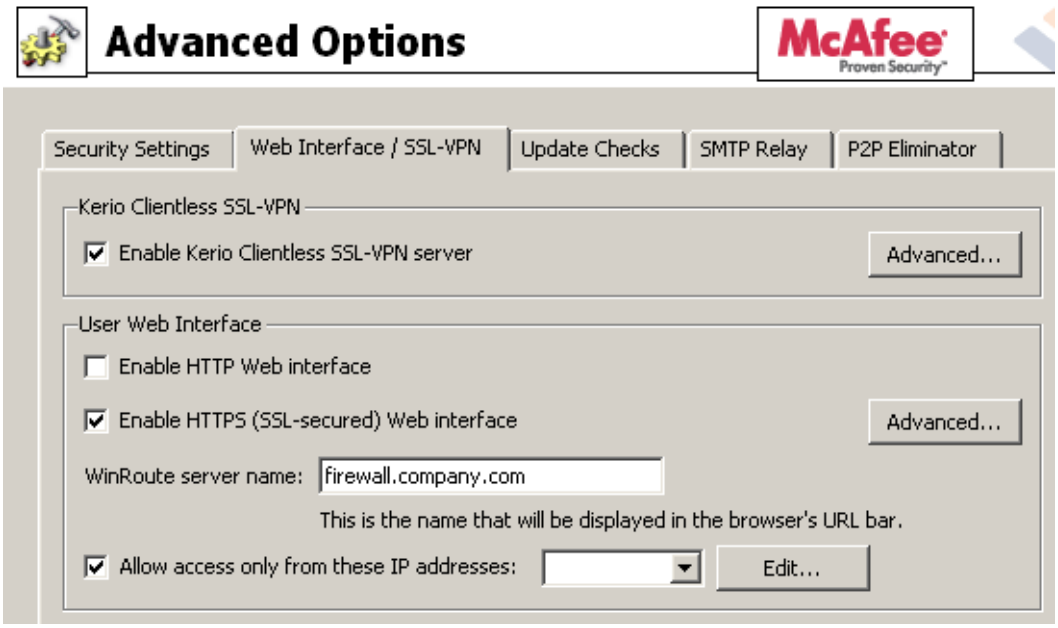


Figure 9.1 Configuration of WinRoute's Web Interface

Enable secured Web Interface (HTTPS)

Use this option to open the secured version (HTTPS) of the Web interface The default port for this interface is 4081.

WinRoute server name

Server DNS name that will be used for purposes of the Web interface (e.g. `server.company.com`). The name need not be necessarily identical with the host name, however, there must exist an appropriate entry in DNS for proper name resolution. The SSL certificate for the secure web interface (see below) should be also issued for the server (i.e. the server name).

The server name is also used in case that *WinRoute* needs redirect the browser to the login page (for example if an unauthenticated user attempts to open a web page where authentication is required — see chapters8.1 and 10.2).

Note: If all clients accessing the Web Interface use the *DNS Forwarder* in *WinRoute* as a DNS server, there is no need to add the server name to DNS. The name is already known and combined with the name of the local domain — see chapter 5.3).

Allow access only from these IP addresses

Select IP addresses which will always be allowed to connect to the Web interface (usually hosts in the local network). You can also click the *Edit* button to edit a selected group of IP addresses or to create a new IP group (details in chapter 12.1).

Note: Access restrictions are applied to both unencrypted and encrypted versions of the Web interface.

Advanced parameters for the Web interface can be set upon clicking on the *Advanced* button.

Configuration of ports of the Web Interface

Use the *TCP ports* section to set ports for unencrypted and encrypted versions of the Web interface (default ports are 4080 for the unencrypted and 4081 for the encrypted version of the Web interface).

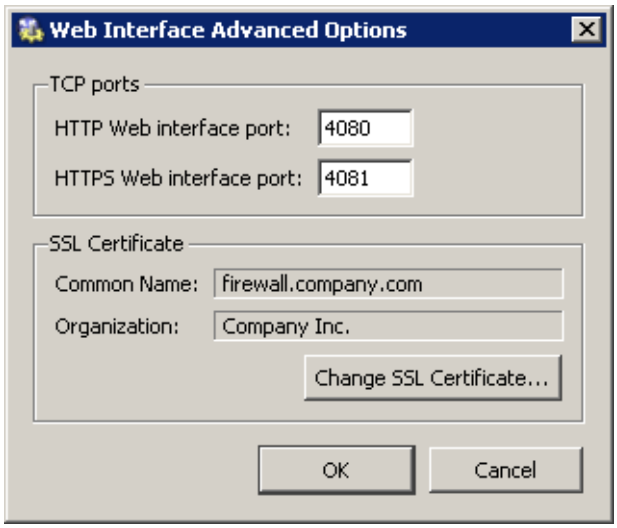


Figure 9.2 Configuration of ports in WinRoute's Web Interface

HINT: If no WWW server is running on the *WinRoute* host, standard port (i.e. 80) for HTTP can be used for the unencrypted Web interface. In such a case, the port number is not necessarily required in URLs for pages of the unencrypted Web interfaces.

Warning: If any of the entries are specified by a port which is already used by another service or application, and the *Apply* button (in *Configuration* → *Advanced Options*) is clicked, *WinRoute* will accept this port, however, the Web interface will not run at the port and an error in the following format will be reported in the *Error* log (see chapter 20.8):

```
Socket error: Unable to bind socket for service to port 80.
  (5002) Failed to start service "WebInterface"
  bound to address 192.168.1.10.
```

If you are not sure that specified ports are free, check the *Error* log immediately after clicking *Apply* to find out whether the corresponding error has been logged.

SSL Certificate for the Web Interface

The principle of an encrypted *WinRoute* Web interface is based on the fact that all communication between the client and server is encrypted to protect it from wiretapping and misuse of the transmitted data. The SSL protocol uses an asymmetric encryption first to facilitate exchange of the symmetric encryption key which will be later used to encrypt the transmitted data.

The asymmetric cipher uses two keys: a public one for encrypting and a private one for decrypting. As their names suggest, the public (encrypting) key is available to anyone wishing to establish a connection with the server, whereas the private (decrypting) key is available only to the server and must remain secret. The client, however, also needs to be able to identify the server (to find out if it is truly the server and not an impostor). For this purpose there is a certificate, which contains the public server key, the server name, expiration date and other details. To ensure the authenticity of the certificate it must be certified and signed by a third party, the certification authority.

Communication between the client and server then follows this scheme: the client generates a symetric enctryption key for and encrypts it with the public server key (obtained from the server certificate). The server decrypts it with its private key (kept solely by the server). Thus the symmetric key is known only to the server and client. This key is then used for encryption and decipher any other traffic.

Generate or Import Certificate

During *WinRoute* installation, a testing certificate for the SSL-secured Web interface is created automatically (it is stored in the `sslcert` subdirectory under the *WinRoute's* installation directory, in the `server.crt` file; the private key for the certificate is saved as `server.key`). The certificate created is unique. However, it is issued against a non-existing server name and it is not issued by a trustworthy certificate authority. This certificate is intended to ensure functionality of the secured Web interface (usually for testing purposes) until a new certificate is created or a certificate issued by a public certificate authority is imported.

Click on the *Change SSL certificate* (in the dialog for advanced settings for the Web interface) to view the dialog with the current server certificate. By selecting the *Field* (certificate entry) option you can view information either about the certificate issuer or about the subject represented by your server.

You can obtain your own certificate, which verifies your server's identity, by two means.

You can create your own self-signed certificate. Click *Generate Certificate* in the dialog where current server status is displayed. Insert required data about the server and your company into the dialog entries. Only entries marked with an asterisk (*) are required.

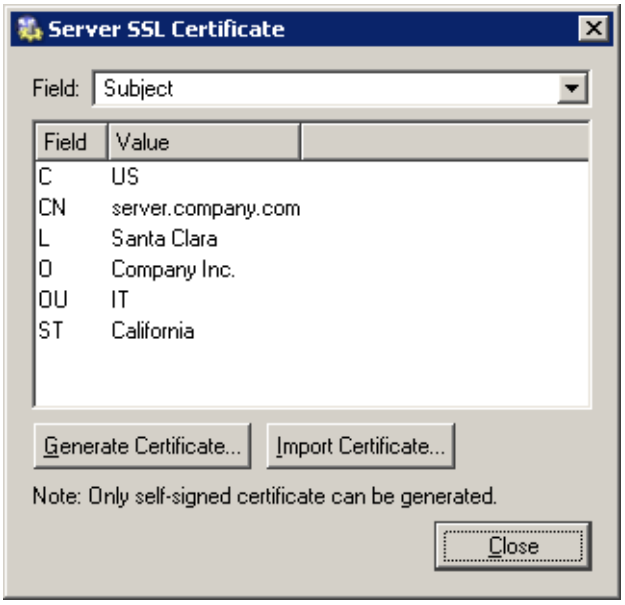


Figure 9.3 SSL certificate of WinRoute's Web interface

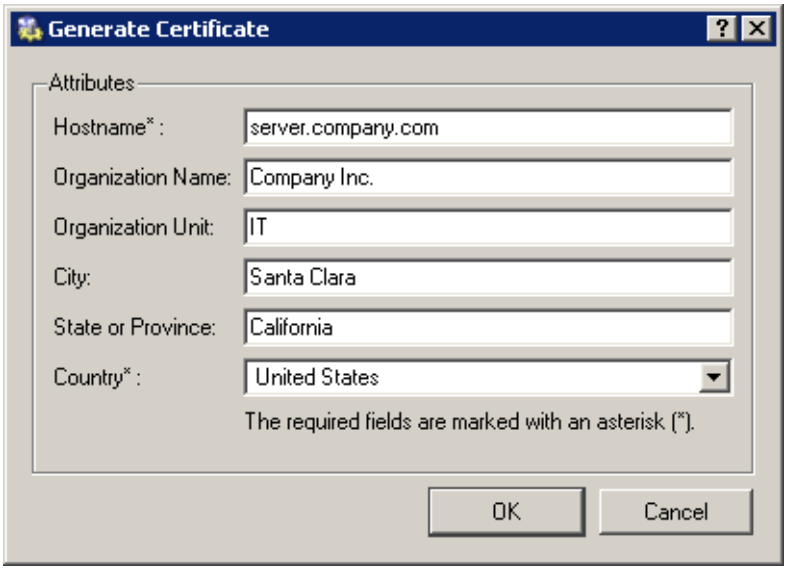


Figure 9.4 Creating a new "self-signed" certificate for WinRoute's Web interface

Click on the *OK* button to view the *Server SSL certificate* dialog. The certificate will be started automatically (you will not need to restart your operating system). When created, the certificate is saved as `server.crt` and the corresponding private key as `server.key`.

A new (*self-signed*) certificate is unique. It is created by your company, addressed to your company and based on the name of your server. Unlike the testing version of the certificate, this certificate ensures your clients security, as it is unique and the identity

of your server is guaranteed by it. Clients will be warned only about the fact that the certificate was not issued by a trustworthy certification authority. However, they can install the certificate in the browser without worrying since they are aware of who and why created the certificate. Secure communication is then ensured for them and no warning will be displayed again because your certificate has all it needs.

The other option is to purchase a signed certificate from a public certificate authority (e.g. Verisign, Thawte, SecureSign, SecureNet, Microsoft Authenticode, etc.).

To import a certificate, open the certificate file (`*.crt`) and the file including the corresponding private key (`*.key`). These files are stored in `sslcert` under the *WinRoute's* installation directory.

The process of certification is quite complex and requires a certain expertise. For detailed instructions contact Kerio technical support.

Web Interface Language Preferences

WinRoute's Web Interface is available in various languages. The language is set automatically according to each users' preferences defined in the Web browser (this function is available in most browsers). English will be used if no preferred language is available .

In the latest *WinRoute*, the Web interface is available in English, Spanish, Czech, Slovak and Russian.

9.2 Login/logout page

User authentication is required for access to the *WinRoute's* web interface. Any user with their own account in *WinRoute* can authenticate to the web interface (regardless their access rights).

Note: Authentication at the web interface is a basic user authentication method at the firewall. Other authentication methods are described in chapter 8.1.

Users logged in

Authentication page through which users login to the firewall against username and password.

Warning:

If more than one *Active Directory* domain are used (see chapter 13.4), the following rules apply to the user name:

Figure 9.5 Login page of the firewall's Web interface

- *User from the local database* — the name must be specified without the domain (e.g. `admin`),
- *Primary domain* — missing domain is acceptable in the name specification (e.g. `jsmith`), but it is also possible to include the domain (e.g. `jsmith@company.com`),
- *Other domains* — the name specified must include the domain

  (e.g. `drdolittle@usoffice.company.com`).

  If none or just one *Active Directory* domain is mapped, all users can authenticate by their usernames without the domain specified.

If the user is re-directed to the page automatically (after inserting the URL of a page for which the firewall authentication is required), he/she will be re-directed to the formerly requested website after successful login attempt. Otherwise, the web interface's welcome page is displayed.

The welcome page varies depending on the rights of the user (see chapter 13.1):

- If the user is allowed to view statistics, the web interface will switch to the *Kerio StaR* mode and it will start with the page of overall statistics (the *overall* tab — for details, see chapter 19). The *My Account* option available at the upper-right corner can be used to switch to the user settings. It is possible to return to the statistics page by the *Statistics* link.

- If the user is not allowed to view statistics, user status info page is displayed instead

(see chapter 9.3).

Log out

Once finished with activities where authentication is required, it is recommended to log out of the firewall by using the *Logout* button. It is important to log out especially when multiple users work at the same host. If a user doesn't log out of the firewall, their identity might be misused easily.

User password authentication

If an access to the web interface is attempted when an authentication from the particular host is still valid (the user has not logged out and the timeout for idleness has not expired — see chapter 9.1) but the particular session[4] has already expired, *WinRoute* requires user authentication by password. This precaution helps avoid misuse of the user identity by another user.

Under such conditions, a special version of the login page is opened.

KerioWinRouteFirewall6
Login Page
Login
The following user is currently logged on from your computer:
John Smith
For security reasons, you have to re-enter your password to access the Kerio Winroute Firewall's Web Interface
Username: jsmith
Password:
Login
Logout this user

Figure 9.6 User authentication by password

[4] *Session* is every single period during which a browser is running. For example, in case of *Internet Explorer*, *Firefox* and *Opera*, a session is terminated whenever all windows and tabs of the browser are closed, while in case of *Netscape/Mozilla/SeaMonkey*, a session is not closed unless the *Quick Launch* program is stopped (an icon is displayed in the toolbar's notification area when the program is running).

Authenticated user connecting to the web interface can continue their work in the interface after entering their password. If a new user attempts to connect to the web interface, the connected user must log out first and then the new user is asked to authenticate by username and password.

9.3 Status information and user statistics

On the *Status* tab, the following information is provided:

User and firewall information

The page header provides user's name or their username as well as the firewall's DNS name or IP address.

Transfer Quota Statistics

The upper section of the *Status* page provides information on the data volume having been transferred by the moment in both directions (download, upload) for the particular day (today), week and month. If a quota is set (see chapter 13.1), information on usage of individual quotas (percentage) is also provided here.
Note: WinRoute does not allow setting of weekly quotas.
TIP: Week and month starting days can be changed in accounting period settings — see chapter 19.2.

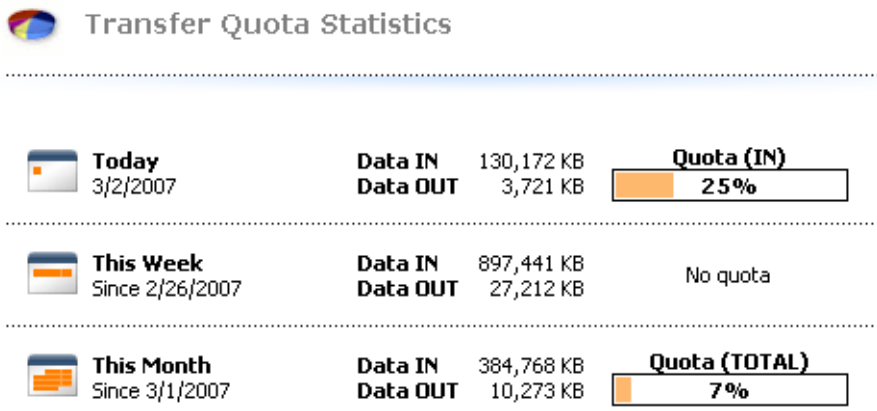


Figure 9.7 Transfer Quota Statistics

Web Site Restrictions

The lower part of the *Status* tab provides an overview of current URL rules applied to the particular user (i.e. rules applied to all users, rules applied to the particular user and rules applied to the group the user belongs to). This makes it simple to find out which web pages and objects are allowed or restricted for the particular user. Time intervals within which the rules are valid are provided as well.

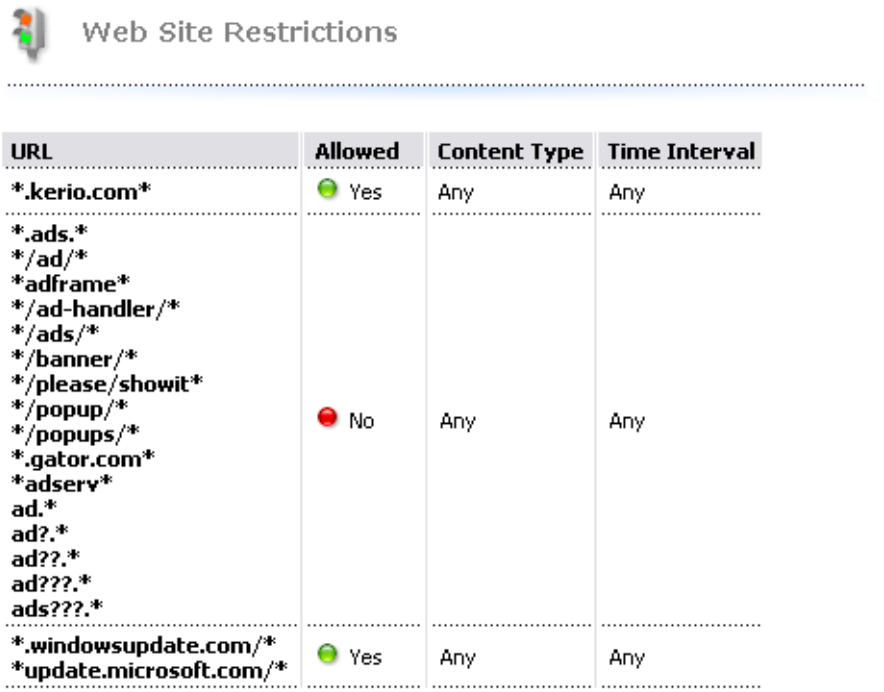


Figure 9.8 Current web restrictions and rules

To learn more details about restriction rules for accessing Web pages refer to chapter 10.2.

9.4 User preferences

The *Preferences* tab allows setting of custom web content filtering and user password.

The upper section of the page enables to permit or deny particular items of web pages.

Content filter options

If the checkbox under a filter is enabled, this feature will be available (it will not be blocked by the firewall).

If a certain feature is disabled in the parameters of a user account (see chapter 13.1), a corresponding item within this page is inactive (user cannot change settings of the item). Users are only allowed to make the settings more restrictive. In other words, users cannot enable an HTML item denied by the administrators for themselves.

- *Java applets* `<applet>` HTML tag blocking
- *ActiveX* — Microsoft ActiveX features (this technology enables, for example, execution of applications at client hosts)
  This option blocks `<object>` and `<embed>` HTML tags
- *Scripts* — `<script>` HTML tag blocking (commands of JavaScript, VBScript, etc.)
- *Pop-up windows* — automatic opening of new windows in the browser (usually advertisements)

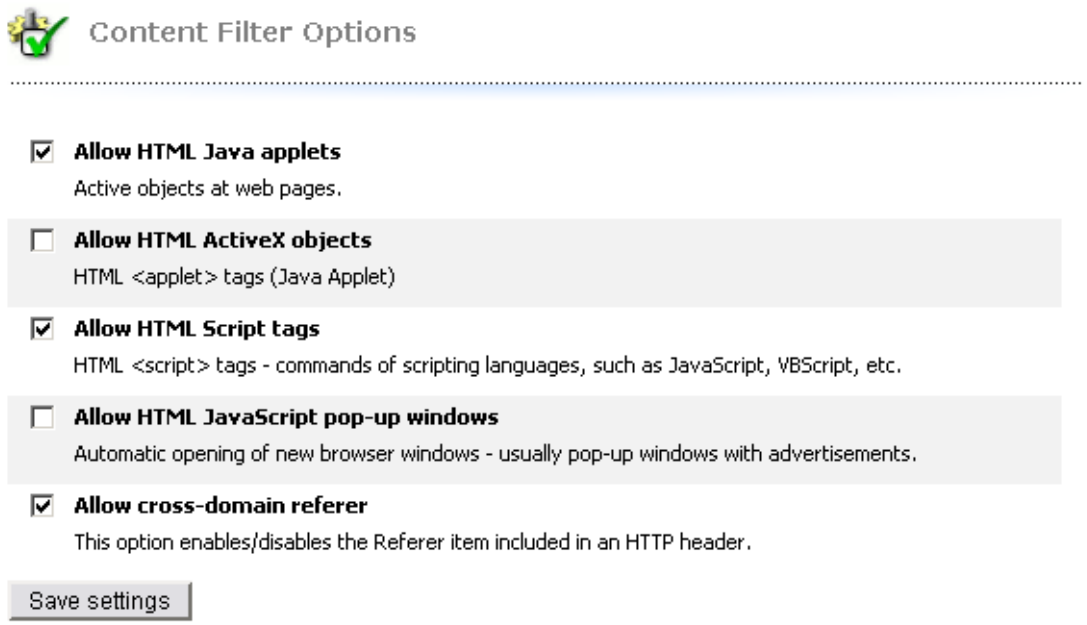

Content Filter Options
Allow HTML Java applets
Active objects at web pages.
Allow HTML ActiveX objects
HTML <applet> tags (Java Applet)
Allow HTML Script tags
HTML <script> tags - commands of scripting languages, such as JavaScript, VBScript, etc.
Allow HTML JavaScript pop-up windows
Automatic opening of new browser windows - usually pop-up windows with advertisements.
Allow cross-domain referer
This option enables/disables the Referer item included in an HTTP header.
Save settings

Figure 9.9 Customized Web objects filtering

This option will block the `window.open()` method in *JavaScript*.

- *Cross-domain referrer* — blocking of the `Referrer` items in HTTP headers.
  This item includes pages that have been viewed prior to the current page. The *Cross-domain referrer* option blocks the `Referrer` item in case this item does not match the required server name.
  Cross-domain referrer blocking protects users' privacy (the `Referrer` item can be monitored to determine which pages are opened by a user).

Save settings

To save and activate settings, click on this button.

Note: Changes in configuration of content filtering in a user account (see chapter 13.1) will take effect upon a next login of the user.

The lower section of the *Preferences* page allows setting of user password.

To change a password, enter the current user password, new password, and the new password confirmation into the appropriate text fields. Save the new password with the *Change password* button.

Warning: Passwords can be changed only if the user is configured in the *WinRoute* internal database (see chapter 13.1). If another authentication method used, the *WinRoute Firewall Engine* will not be allowed to change the password. In such a case, the *Change password* section is not even displayed in the *Preferences* page.

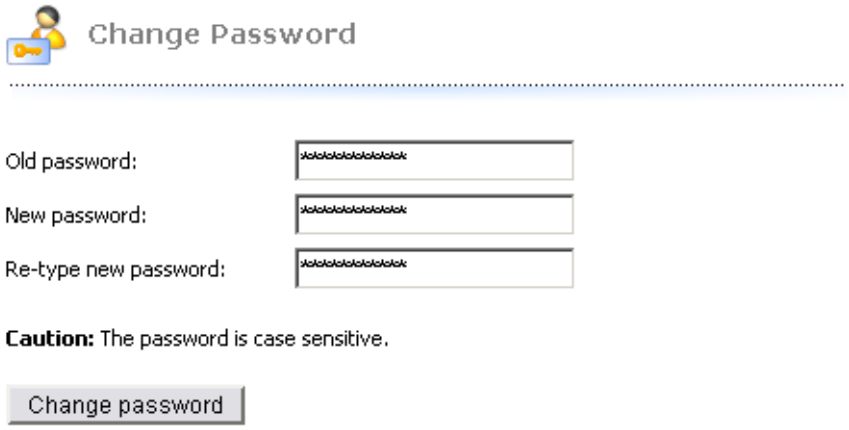


Figure 9.10 Editing user password

Chapter 10

HTTP and FTP filtering

WinRoute provides a wide range of features to filter traffic using HTTP and FTP protocols. These protocols are the most spread and the most used in the Internet.

Here are the main purposes of HTTP and FTP content filtering:

- to block access to undesirable Web sites (i.e. pages that do not relate to employees' work)
- to block certain types of files (i.e. illegal content)
- to block or to limit viruses, worms and Trojan horses

Let's focus on filtering options featured by *WinRoute*. For their detailed description, read the following chapters.

HTTP protocol

— Web pages filtering:

- access limitations according to URL (substrings contained in URL addresses)
- blocking of certain HTML items (i.e. scripts, ActiveX objects, etc.)
- filtering based on classification by the *ISS OrangeWeb Filter* module (worldwide Website classification database)
- limitations based on occurrence of denied words (strings)
- antivirus control of downloaded objects

FTP protocol

— control of access to FTP servers:

- access to certain FTP servers is denied
- limitations based on or file names
- transfer of files is limited to one direction only (i.e. download only)
- certain FTP commands are blocked
- antivirus control of transferred files

Note: WinRoute provides only tools for filtering and access limitations. Decisions on which websites and files will be blocked must be made by the administrator (or another qualified person).

10.1 Conditions for HTTP and FTP filtering

For HTTP and FTP content filtering, the following conditions must be met:

1. Traffic must be controlled by an appropriate protocol inspector.

   An appropriate protocol inspector is activated automatically unless its use is denied by traffic rules. For details, refer to chapter 6.3.

2. Connections must not be encrypted. SSL encrypted traffic (HTTPS and FTPS protocols) cannot be monitored. In this case you can block access to certain servers using traffic rules (see chapter 6.3).

3. FTP protocols cannot be filtered if the secured authentication (*SASO*) is used.

4. Both HTTP and FTP rules are applied also when the *WinRoute's* proxy server is used (then, condition 1 is irrelevant). However, FTP protocol cannot be filtered if the parent proxy server is used (for details, see chapter 5.5). In such a case, FTP rules are not applied.

5. If the proxy server is used (see chapter 5.5), It is also possible to filter HTTPS servers (e.g. `https://secure.kerio.com/`). However, it is not possible to filter individual objects at these servers.

10.2 URL Rules

These rules allow the administrator to limit access to Web pages with URLs that meet certain criteria. They include other functions, such as filtering of web pages by occurrence forbidden words, blocking of specific items (scripts, active objects, etc.) and antivirus switch for certain pages.

To define URL rules, go to the *URL Rules* tab in *Configuration* → *Content Filtering* → *HTTP Policy*.

Rules in this section are tested from the top of the list downwards (you can order the list entries using the arrow buttons at the right side of the dialog window). If a requested URL passes through all rules without any match, access to the site is allowed. All URLs are allowed by default (unless denied by a URL rule).

Note: URLs which do not match with any URL rule are available for any authenticated user (any traffic permitted by default). To allow accessing only a specific web page group

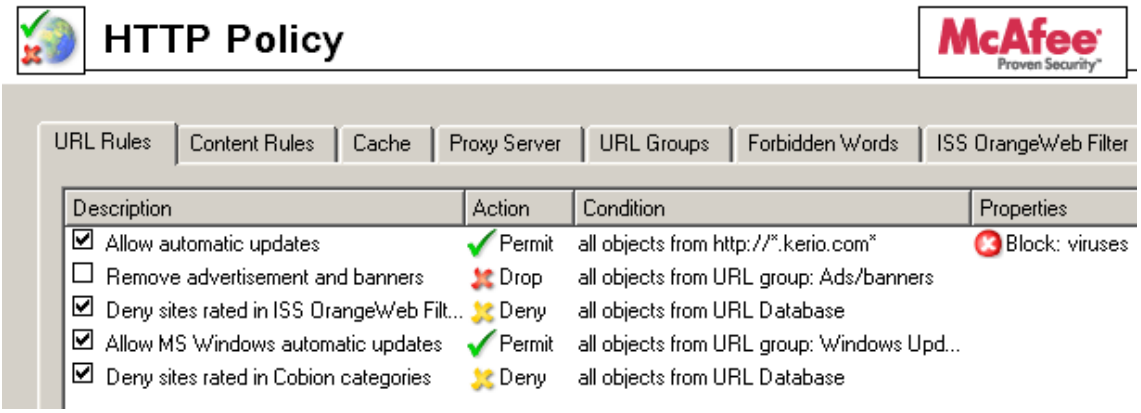


Figure 10.1 URL Rules

and block access to other web pages, a rule denying access to any URL must be placed at the end of the rule list.

The following items (columns) can be available in the *URL Rules* tab:

- *Description* — description of a particular rule (for reference only). You can use the checking box next to the description to enable/disable the rule (for example, for a certain time).
- *Action* — action which will be performed if all conditions of the rule are met (*Permit* — access to the page will be allowed, *Deny* — connection to the page will be denied and denial information will be displayed, *Drop* — access will be denied and a blank page will be opened, *Redirect* — user will be redirected to the page specified in the rule).
- *Condition* — condition which must be met to apply the rule (e.g. URL matches certain criteria, page is included in a particular category of the *ISS OrangeWeb Filter* database, etc.).
- *Properties* — advanced options for the rule (e.g. anti-virus check, content filtering, etc.).

The following columns are hidden by default. To view them, use the *Modify columns* function in the context menu — for details, see chapter 3.2.

- *IP Groups* — IP group to which the rule is applied. The IP groups include addresses of clients (workstations of users who connect to the Internet through *WinRoute*).
- *Valid Time* — time interval during which the rule is applied.
- *Users List* — list of users and user groups to which the rule applies.

Note: The default *WinRoute* installation includes several predefined URL rules. These rules are disabled by default. These rules are available to the *WinRoute* administrators.

URL Rules Definition

To create a new rule, select a rule after which the new rule will be added, and click *Add*. You can later use the arrow buttons to reorder the rule list.

Use the *Add* button to open a dialog for creating a new rule.

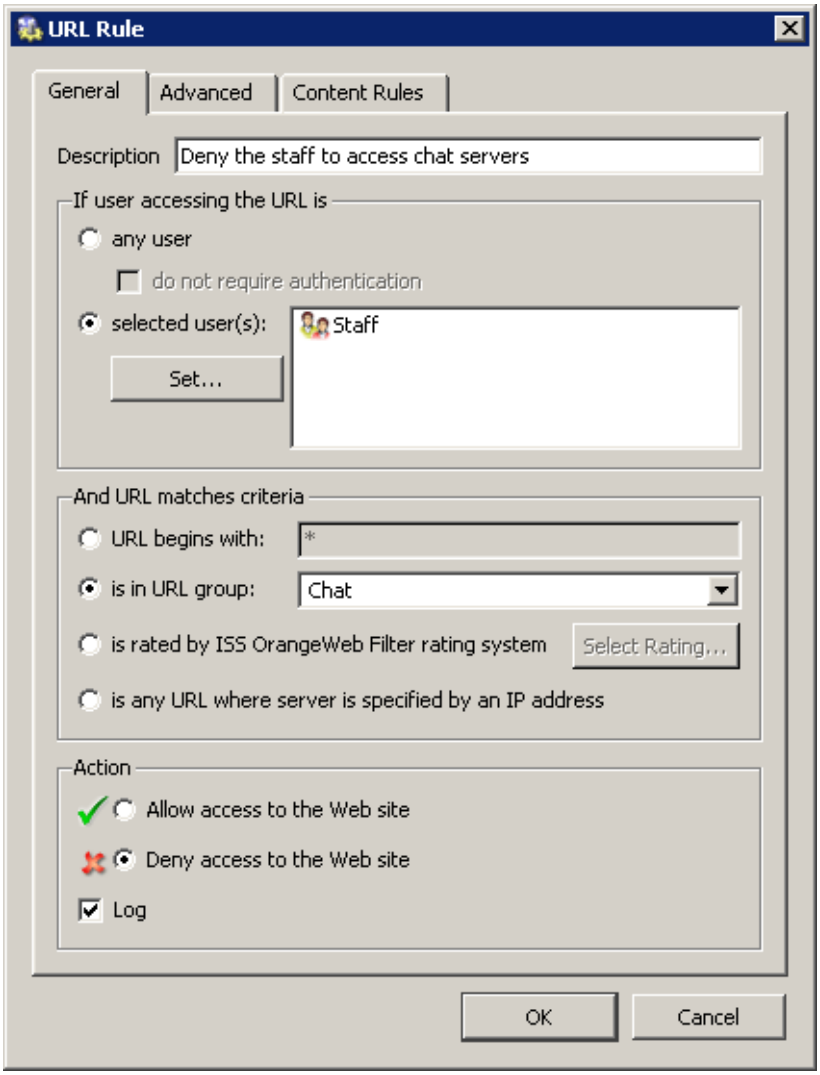


Figure 10.2 URL Rule — basic parameters

Open the *General* tab to set general rules and actions to be taken.

Description
Description of the rule (information for the administrator).

If user accessing the URL is
Select which users this rule will be applied on:

- *any user* — for all users (no authentication required).
  selected user(s) — for selected users or/and user groups who have authenticated to the firewall.
  Notes:
  1. It is often desired that the firewall requires user authentication before letting them open a web page. This can be set on the *Authentication Options* tab in *Users* (refer to chapter 13.1). Using the *do not require authentication* option, for example a rule allowing access to certain pages without authentication can be defined.
  2. Unless authentication is required, the *do not require authentication* option is ineffective.
- *selected user(s)* — applied on selected users or/and user groups.
  Click on the *Set* button to select users or groups (hold the *Ctrl* and the *Shift* keys to select more that one user /group at once).
  Note: In rules, username represents IP address of the host fro which the user is currently connected to the firewall (for details, see chapter 8.1).

And URL matches criteria
Specification of URL (or URL group) on which this rule will be applied:

- *URL begins with* — this item can include either entire URL (i.e. `www.kerio.com/index.html`) or only a substring of a URL using an asterisk (wildcard matching) to substitute any number of characters (i.e. `*.kerio.com*`) Server names represent any URL at a corresponding server (`www.kerio.com/*`).
- *is in URL group* — selection of a URL group (refer to chapter 12.4) which the URL should match with
- *is rated by ISS OrangeWeb Filter rating system* — the rule will be applied on all pages matched with a selected category by the *ISS OrangeWeb Filter* plug-in (see chapter 10.4).
  Click on the *Select Rating...* button to select from *ISS OrangeWeb Filter* categories. For details, refer to chapter 10.4.
- *is any URL where server is given as IP address* — by enabling this option users will not be able to bypass URL based filters by connecting to Web sites by IP address rather than domain name. This trick is often used by servers offering illegal downloads.

Warning: If access to servers specified by IP addresses is not denied, users can bypass URL rules where servers are specified by names.

Action

Selection of an action that will be taken whenever a user accesses a URL meeting a rule:

- *Allow access to the Web site*
- *Deny access to the Web site* — requested page will be blocked. The user will be informed that the access is denied or a blank page will be displayed (according to settings in the *Advanced* tab — see below).

Tick the *Log* option to log all pages meeting this rule in the *Filter* log (see chapter 20.9).

Go to the *Advanced* tab to define more conditions for the rule or/and to set options for denied pages.

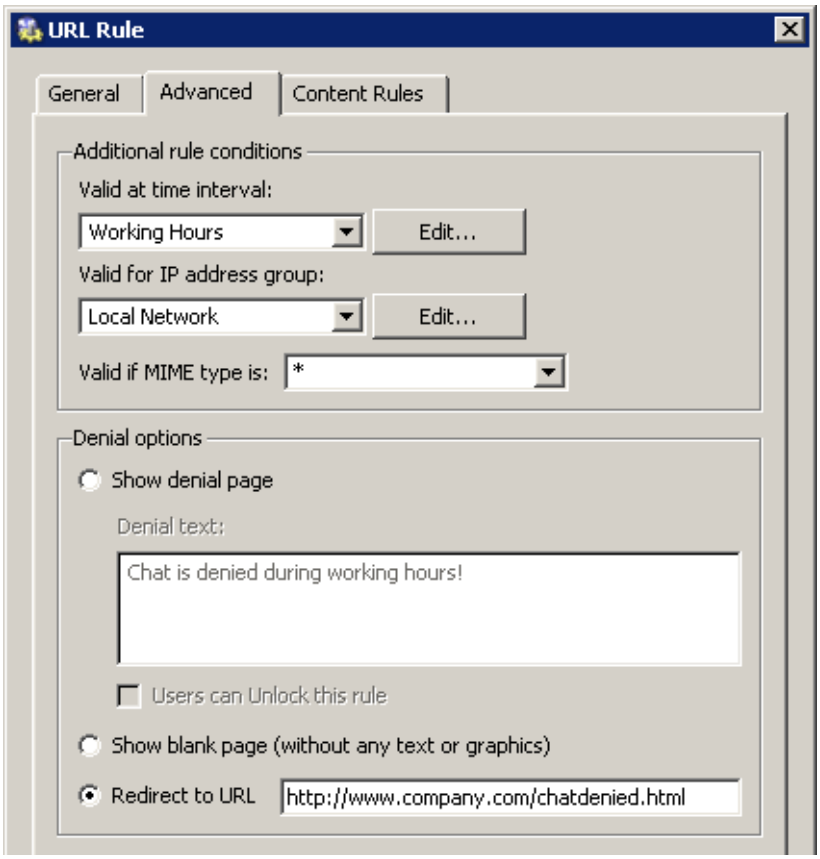


Figure 10.3 URL Rule — advanced parameters

Valid at time interval

Selection of the time interval during which the rule will be valid (apart from this interval the rule will be ignored). Use the *Edit* button to edit time intervals (for details see chapter 12.2).

Valid for IP address group

Selection of IP address group on which the rule will be applied. Client (source) addresses are considered. Use the *Any* option to make the rule independent of clients.

Click on the *Edit* button to edit IP groups (for details see chapter 12.1).

Valid if MIME type is

The rule will be valid for a certain MIME type only (for example, `text/html` — HTML documents, `image/jpeg` — images in the JPEG format, etc.).

You can either select one of the predefined MIME types or define a new one. An asterisk substitutes any subtype (i.e. `image/*`). An asterisk stands for any MIME type — the rule will be independent of the MIME type.

Denial options

Advanced options for denied pages. Whenever a user attempts to open a page that is denied by the rule, *WinRoute* will display:

- a page informing the user that access to the required page is denied as it is blocked by the firewall. This page can also include an explanation of the denial (the *Denial text* item).

  The *Unlock* button will be displayed in the page informing about the denial if the *Users can Unlock this rule* is ticked. Using this button users can force *WinRoute* to open the required page even though this site is denied by a URL rule. The page will be opened for 10 minutes. Each user can unlock a limited number of denied pages (up to 10 pages at once). All unlocked pages are logged in the *Filter* log (see chapter 20.9).

  Notes:

  1. Only subscribed users are allowed to unlock rules.
  2. If any modifications are done within URL rules, all unlock rules are removed immediately.
- a blank page — user will not be informed why access to the required page was denied.
- another page — user's browser will be redirected to the specified URL. This option can be helpful for example to define a custom page with a warning that access to the particular page is denied.

Open the *Content Rules* tab (in the *HTTP Rules* section) to specify details for content filter rules. Parameters on this tab can be modified only for rules where the *Allow access to the Web site* option is enabled.

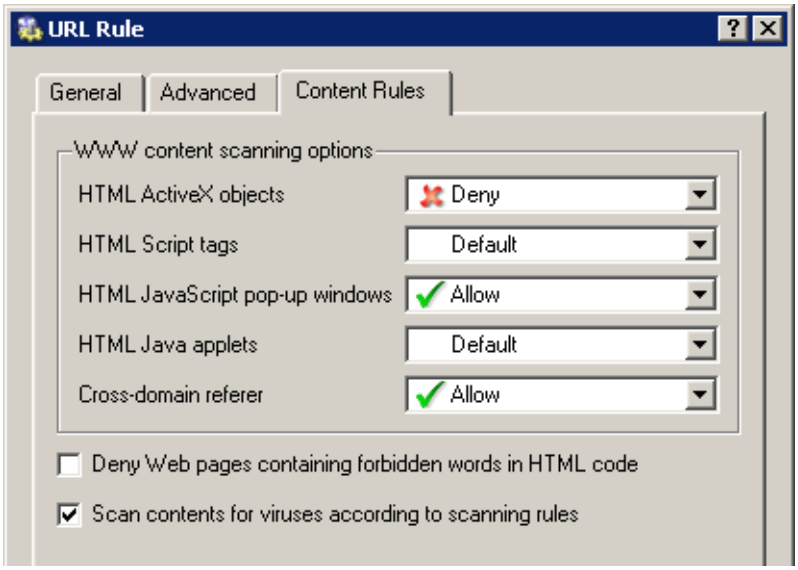


Figure 10.4 Options for Websites with content meeting a URL rule

WWW content scanning options

In this section you can define advanced parameters for filtering of objects contained in Web pages which meet the particular rule (for details refer to chapter 10.3). Specific URL settings have higher priority than user settings (see chapter 13.1) and global rules for unauthorized users (refer to chapter 10.3).
One of the following alternatives can be set for each object type:

- *Allow* — these objects will be displayed.
- *Deny* — these objects will be filtered out of the page
- *Default* — global rules or custom rules of a particular user will be applied to such objects (this implies that this rule will not affect filtering of such objects)

Deny Web pages containing ...

Use this option to deny users to access Web pages containing words/strings defined on the *Forbidden Words* tab in the *Configuration/Content Filtering → HTTP Policy*.
For detailed information on forbidden words, see chapter 10.5.

Scan content for viruses according to scanning rules

Antivirus check according to settings in the *Configuration → Content Filtering → Antivirus* section will be performed (see chapter 11.3) if this option is enabled.

HTTP Inspection Advanced Options

Click on the *Advanced* button in the *HTTP Policy* tab to open a dialog where parameters for the HTTP inspection module can be set.

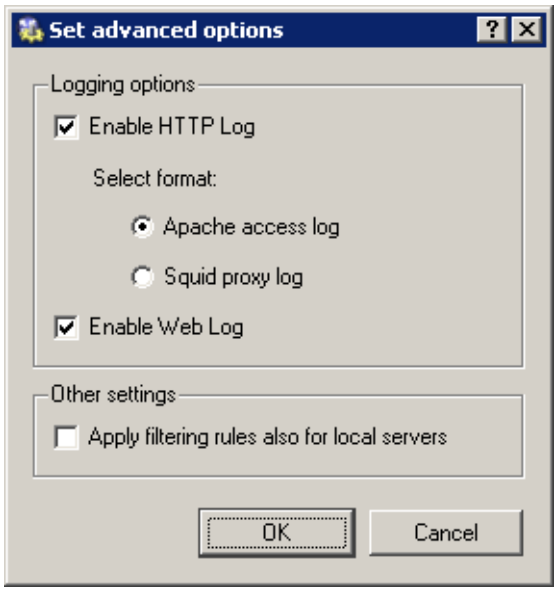


Figure 10.5 HTTP protocol inspector settings

Use the *Enable HTTP Log* and *Enable Web Log* options to enable/disable logging of HTTP queries (opened web pages) to the *HTTP* log (see chapter 20.10) and to the *Web* log (refer to chapter 20.14).

Log format can be chosen for the *Enable HTTP Log* item: *Apache* access log (`http://www.apache.org/`) or *Squid* proxy log (`http://www.squid-cache.org/`). This may be important especially when the log would be processed by a specific analysis tool.

Both *HTTP* and *Web* logs are enabled by default. The *Apache* option is selected by default for its better reference.

Use the *Apply filtering rules also for local server* to specify whether content filtering rules will be applied to local WWW servers which are available from the Internet (see chapter 6). This option is disabled by default — the protocol inspector only scans HTTP protocol syntax and performs logging of queries (WWW pages) according to the settings.

10.3 Global rules for Web elements

In *WinRoute* you can also block certain features contained in HTML pages. Typical undesirable items are ActiveX objects (they might enable starting of applications on client hosts) and pop-up windows (automatically opened browser windows, usually used for advert purposes).

To define content global filtering rules go to the *Content Rules* tab in the *Configuration* → *Content Filtering* → *HTTP Policy* section. Special settings for individual pages can be defined in URL Rules section (refer to chapter 10.2).

Settings on the *WWW content scanning options* tab are applied to traffic of hosts where users are not authenticated. Special settings are used for users connected through the firewall.

Each authenticated user can customize filtering rules at the user preferences page (see chapter 9.4). However, users that are not allowed to *override WWW content rules* (refer to chapter 13.1) cannot permit HTML features that are denied globally.

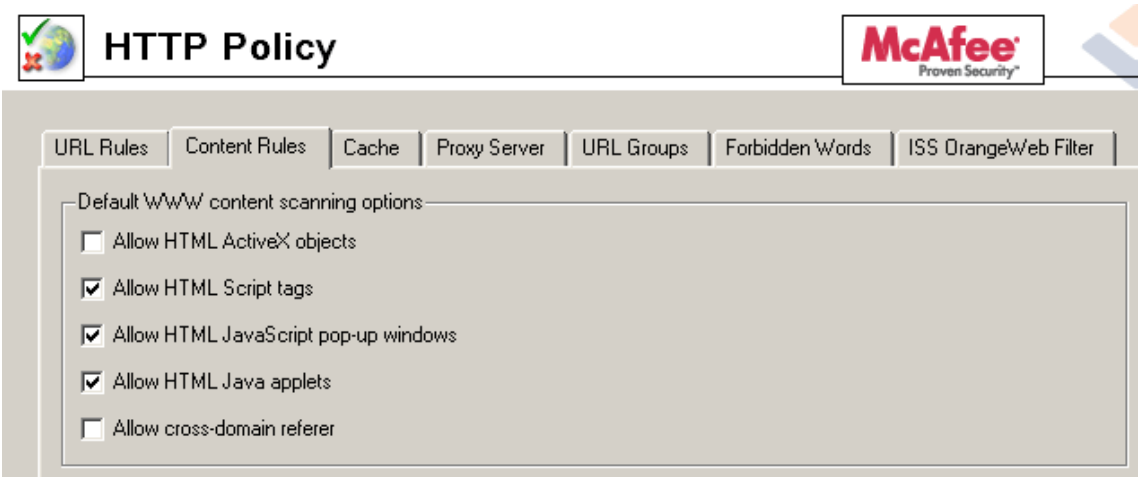


Figure 10.6 Global rules for Web elements

Allow HTML ActiveX objects

Active objects at web pages.

This option allows/blocks `<object>` and `<embed>` HTML tags.

Allow <Script> HTML tags

HTML `<script>` tags — commands of scripting languages, such as *JavaScript*, *VBScript*, etc.

Allow HTML JavaScript pop-up windows

Automatic opening of new browser windows — usually pop-up windows with advertisements.

This option enables/blocks the `window.open()` method in scripts

Allow <applet> HTML tags

HTML `<applet>` tags (*Java Applet*)

Allow cross-domain referrer

This option enables/disables the `Referrer` item included in an HTTP header.

The `Referer` item includes pages that have been viewed prior to the current page.

If the *Allow inter-domain referrer* is off, `Referrer` items that include a server name different from the current HTTP request will be blocked.

The *Cross-domain referrer* function protects users' privacy (the `Referrer` item can be monitored to see which pages are opened by each user).

10.4 Content Rating System (ISS OrangeWeb Filter)

The *ISS OrangeWeb Filter* module enables *WinRoute* to rate Web page content. Each page is sorted into predefined categories. Access to the page will be either permitted or denied according to this classification.

ISS OrangeWeb Filter uses a dynamic worldwide database which includes URLs and classification of Web pages. This database is maintained by special servers that perform page ratings. Whenever a user attempts to access a Web page, *WinRoute* sends a request on the page rating. According to the classification of the page the user will be either allowed or denied to access the page. To speed up URL rating the data that have been once acquired can be stored in the cache and kept for a certain period.

Notes:

1. The *ISS OrangeWeb Filter* module was designed and tested especially on pages in English. Efficiency of its appliance on non-English pages is lower (about 70 % of the full efficiency).

2. A special license is associated with *ISS OrangeWeb Filter*. Unless *WinRoute* includes an *ISS OrangeWeb Filter* license, then the module behaves as a trial version only (this means that it is automatically disabled after 30 days from the *WinRoute* installation and options in the *ISS OrangeWeb Filter* tab will not be available). For detailed information about the licensing policy, read chapter 44.

3. If the Internet connection is provided by a dial-up, it is not recommended to use *ISS OrangeWeb Filter*.

Upon startup of the *WinRoute Engine*, access to the database server is checked (this process is called activation). This activation is refreshed regularly.

If the line is hung up while the activation is being started and refreshed, the activation is not started and the *ISS OrangeWeb Filter* module will not work. In addition, communication with the database server significantly increases the response time for connection to such web pages classification of which is not saved in the local cache.

ISS OrangeWeb Filter configuration

The *ISS OrangeWeb Filter* module can be set and configured through the *ISS OrangeWeb Filter* tab in *Configuration* → *Content Filtering* → *HTTP Policy*.

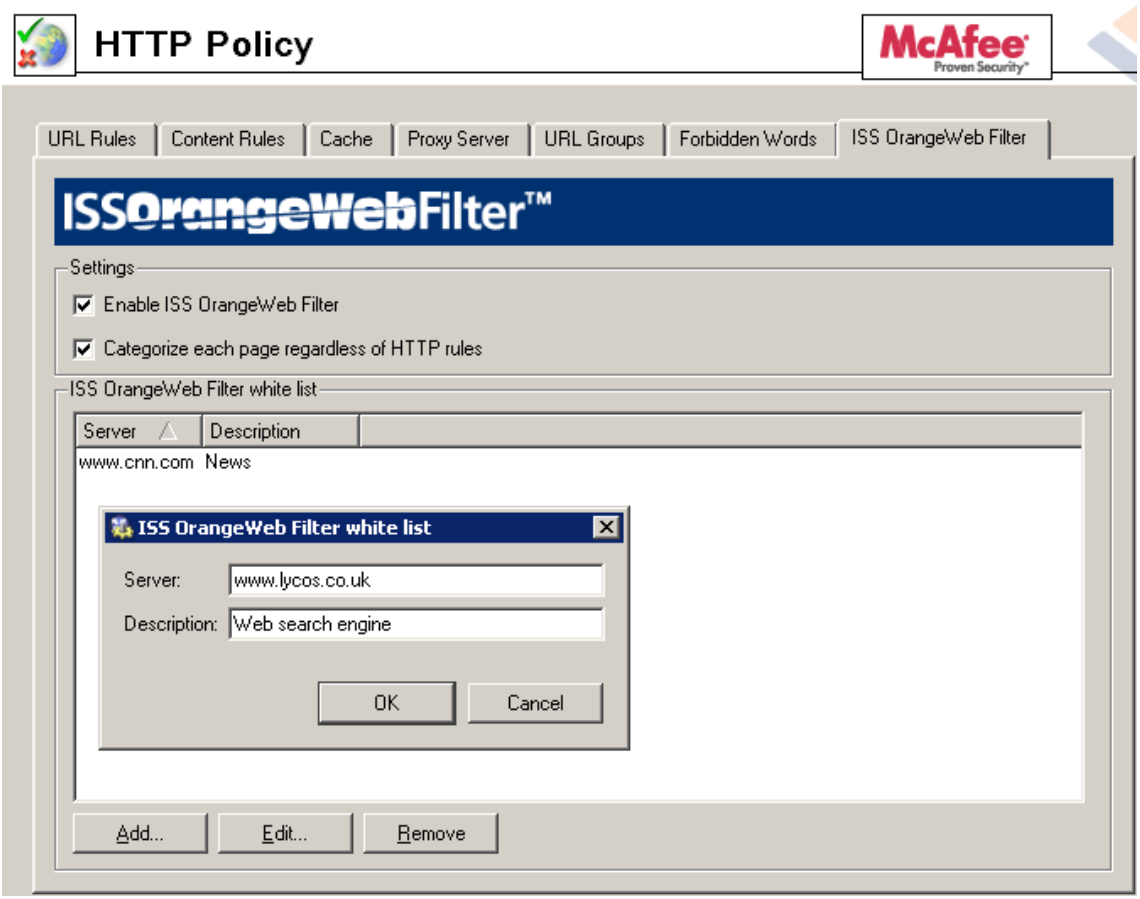


Figure 10.7 ISS OrangeWeb Filter configuration

Enable ISS OrangeWeb Filter

use this option to enable/disable the *ISS OrangeWeb Filter* module for classification of websites.
If *ISS OrangeWeb Filter* is disabled:

- the other options in the *ISS OrangeWeb Filter* tab are not available,
- all URL rules which use the *ISS OrangeWeb Filter* classification are disabled (for details, refer to chapter 10.4).

Categorize each page regardless of HTTP rules

If this option is enabled, *ISS OrangeWeb Filter* categorization will be applied to any web pages (i.e. to all HTTP requests processed by the *HTTP* protocol inspector).
Categorization of all pages is necessary for statistics of the categories of visited web pages (see chapter 19). If you do not intend to keep these statistics, it is recommended disable this option (categorization of all web pages might be demanding and it might decrease *WinRoute* performance).

Servers (Web sites) not to be rated by the module can eb specified in *ISS OrangeWeb Filter white list*. Use the *Add* button to open a dialog where a new item (server or a Web page) can be added.

Server

Use the *Server* item to specify Web sites not to be classified by the *ISS OrangeWeb Filter*. The following items can be specified:

- server name (e.g. `www.kerio.com`). Server name represents any URL at a corresponding server.
- a particular URL (e.g. `www.kerio.com/index.html`). It is not necessary to include protocol specification (`http://`) .
- URL using wildcard matching (e.g. `*.ker?o.*`). An asterisk stands for any number of characters (even zero), a`*.ker?o.*` question-mark represents just one symbol.

Description

Comments for the items defined. For reference only.

ISS OrangeWeb Filter Deployment

To enable classification of Websites by the *ISS OrangeWeb Filter* module, this module must be running and all corresponding parameters must be set.

Whenever *WinRoute* processes a URL rule that requires classification of pages, the *ISS OrangeWeb Filter* plug-in is activated. The usage will be better understood through the following example that describes a rule denying all users to access pages containing job offers.

the following rule has been defined in the *URL Rules* tab in *Configuration* → *Content Filtering* → *HTTP Rules*:

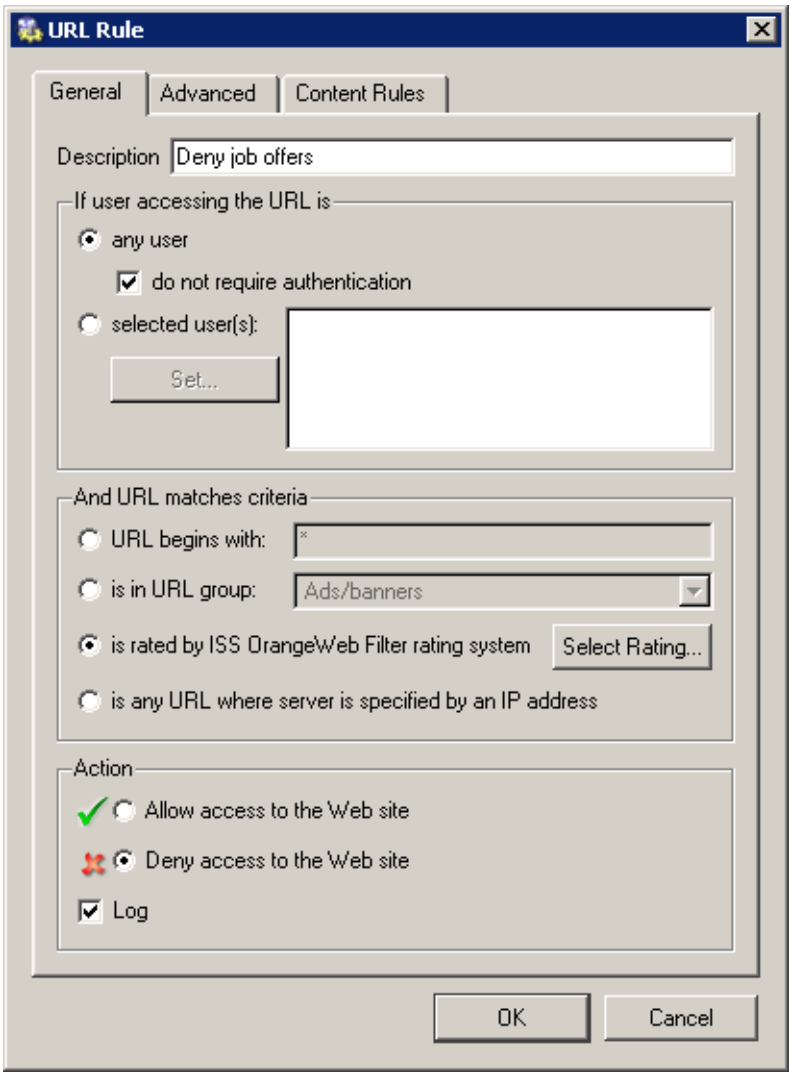


Figure 10.8 ISS OrangeWeb Filter rule

The *is rated by ISS OrangeWeb Filter rating system* is considered the key parameter. The URL of each opened page will be rated by the *ISS OrangeWeb Filter* module. Access to each page matching with a rating category included in the database will be denied.

Use the *Select Rating* button to open a dialog where *ISS OrangeWeb Filter* rating categories can be chosen. Select the *Job Search* rating category (pages including job offers).

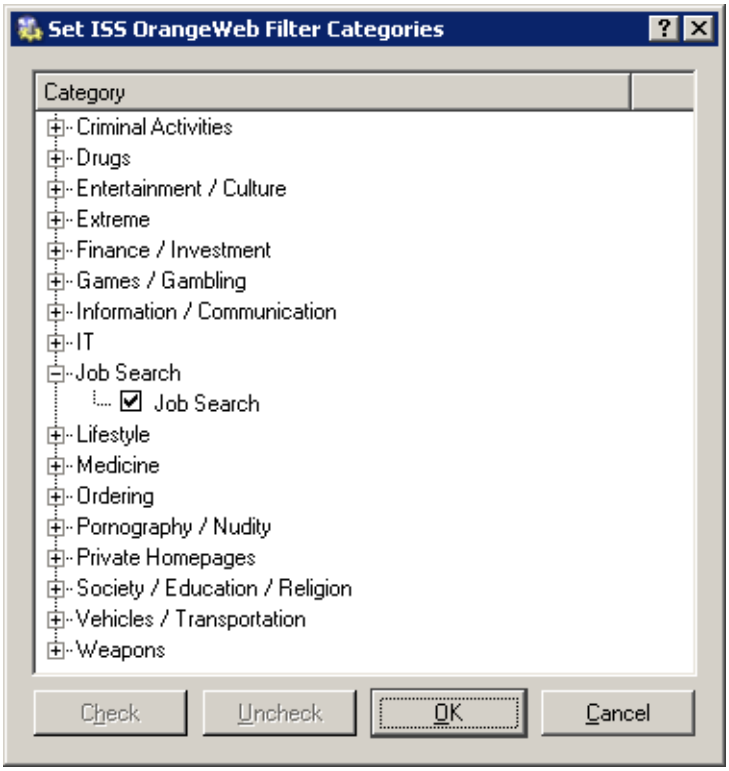


Figure 10.9 ISS OrangeWeb Filter categories

Notes:

1. Use the *Check* button to check all items included in the selected category. You can uncheck all items in the category by clicking *Uncheck*.

2. We recommend you to unlock rules that use the *ISS OrangeWeb Filter* rating system (the *Users can Unlock this rule* option in the *Advanced* tab). This option will allow users to unlock pages blocked for incorrect classification.

10.5 Web content filtering by word occurrence

WinRoute can also filter Web pages that include undesirable words.

This is the filtering principle: Denied words are matched with values, called weight (represented by a whole positive integer). Weights of these words contained in a required page are summed (weight of each word is counted only once regardless of how many times the word is included in the page). If the total weight exceeds the defined limit (so called treshold value), the page is blocked.

So called forbidden words are used to filter out web pages containing undesirable words. URL rules (see chapter 10.2) define how pages including forbidden content will be handled.

Warning: Definition of forbidden words and treshold value is ineffective unless corresponding URL rules are set!

Definition of rules filtering by word occurrence

First, suppose that some forbidden words have been already defined and a treshold value has been set (for details, see below).

On the *URL Rules* tab under *Configuration* → *Content Filtering* → *HTTP Policy*, create a rule (or a set of rules) to allow access to the group of web pages which will be filtered by forbidden words. Go to the *Content Rules* tab under *HTTP Rule* to enable the web content filter.

Example: A rule that will filter all web sites by occurrence of forbidden words.

On the *General* tab, allow all users to access any web site.

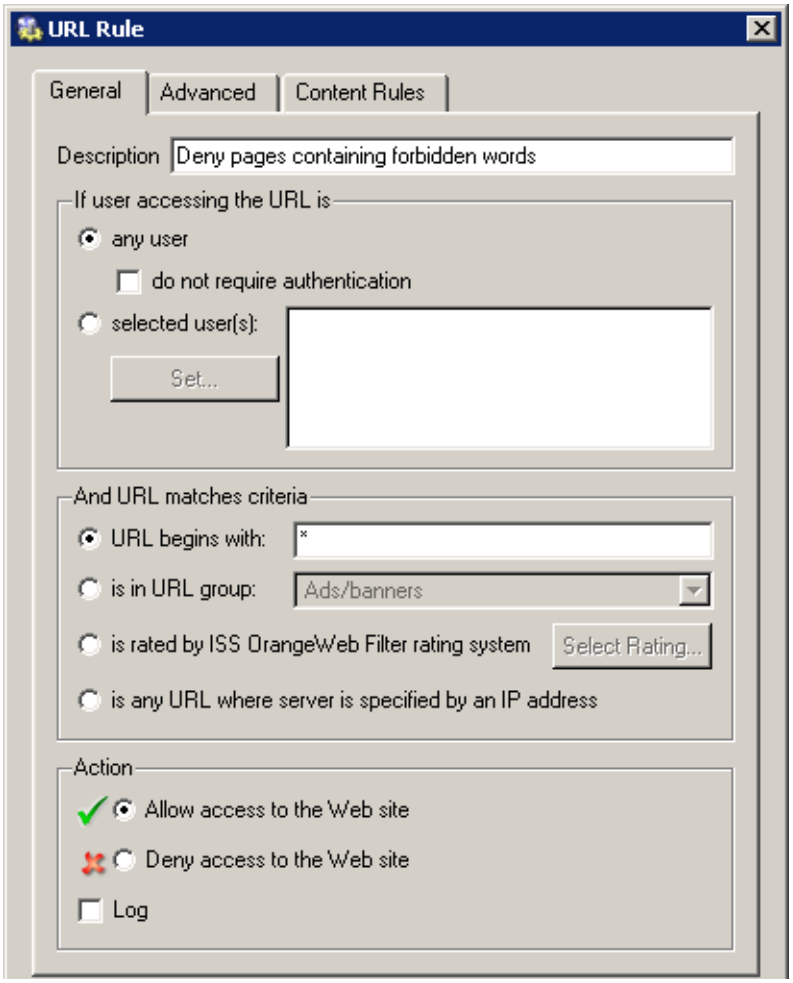


Figure 10.10 A rule filtering web pages by word occurrence (allow access)

On the *Content Rules* tab, check the *Deny Web pages containing...* option to enable filtering by word occurrence.

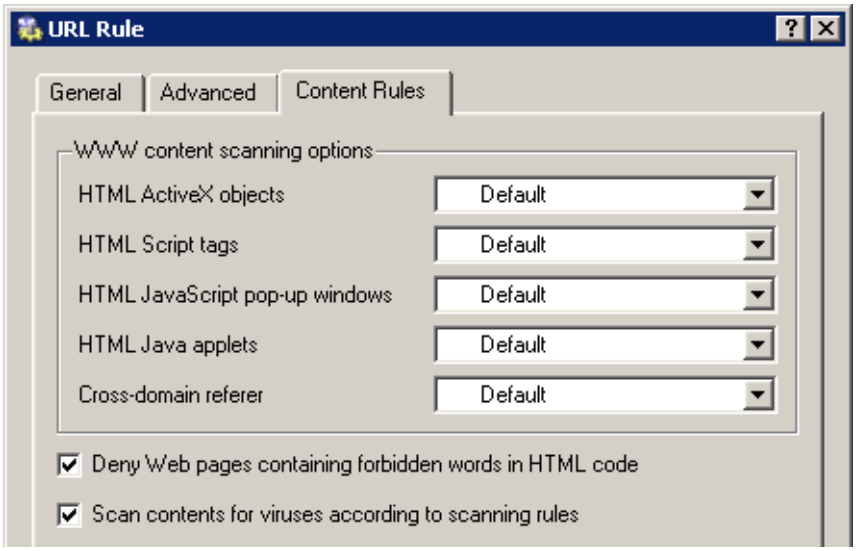


Figure 10.11 A rule filtering web pages by word occurrence (word filtering)

Word groups

To define word groups go to the *Word Groups* tab in *Configuration* → *Content Filtering* → *HTTP Policy*, the *Forbidden Words* tab. Words are sorted into groups. This feature only makes *WinRoute* easier to follow. All groups have the same priority and all of them are always tested.

Individual groups and words included in them are displayed in form of trees. To enable filtering of particular words use checkboxes located next to them. Unchecked words will be ignored. Due to this function it is not necessary to remove rules and define them again later.

Note: The following word groups are predefined in the default *WinRoute* installation:

- *Pornography* — words that typically appear on pages with erotic themes,
- *Warez / Cracks* — words that typically appear on pages offering downloads of illegal software, license key generators etc.

All key words in predefined groups are disabled by default. A *WinRoute* administrator can enable filtering of the particular words and modify the weight for each word.

Treshold value for Web page filtering

The value specified in *Deny pages with weight over* represents so called treshold weight value for each page (i.e. total weight of all forbidden words found at the

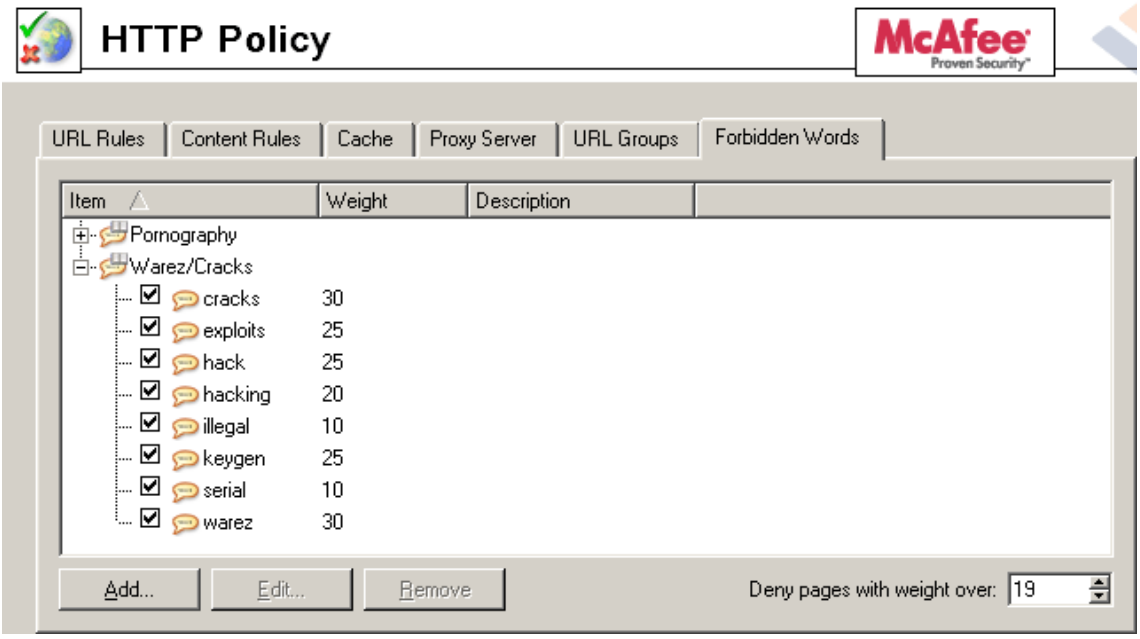


Figure 10.12 Groups of forbidden words

page). If the total weight of the tested page exceeds this limit, access to the page will be denied (each word is counted only once, regardless of the count of individual words).

Definition of forbidden words

Use the *Add* button to add a new word into a group or to create a new group.

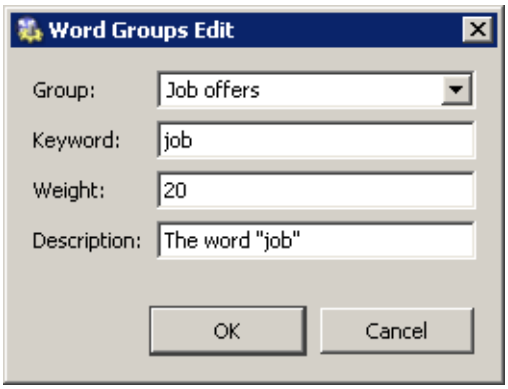


Figure 10.13 Definition of a forbidden word or/and a word group

Group
Selection of a group to which the word will be included. You can also add a new name to create a new group.

Keyword
Forbidden word that is to be scanned for

Weight
Word weight (affects decision about the page denial)

Description
A comment on the word or group.

10.6 FTP Policy

To define rules for access to FTP servers go to *Configuration* → *Content Filtering* → *FTP Rules*.

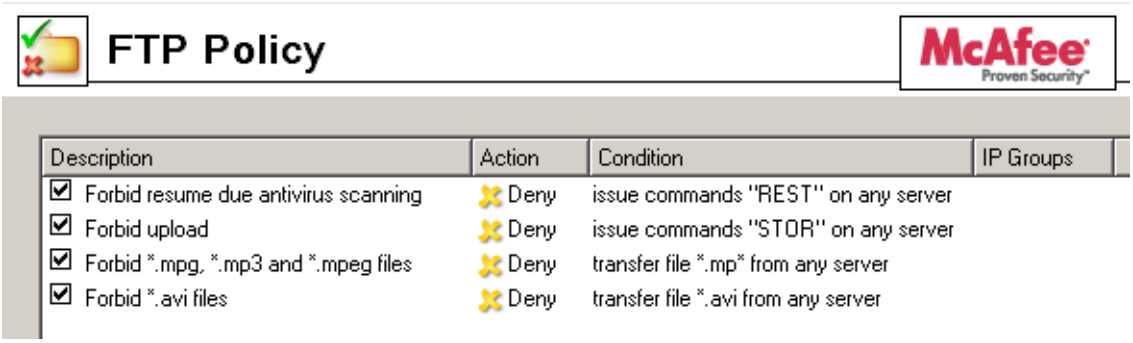


Figure 10.14 FTP Rules

Rules in this section are tested from the top of the list downwards (you can order the list entries using the arrow buttons at the right side of the dialog window). Testing is stopped when the first convenient rule is met. If the query does not match any rule, access to the FTP server is implicitly allowed.

Notes:

1. The default *WinRoute* configuration includes a set of predefined rules for FTP traffic. These rules are disabled by default. These rules are available to the *WinRoute* administrators.

2. A rule which blocks completion of interrupted download processes (so called *resume* function executed by the `REST` FTP command). This function is essential for proper functionality of the antivirus control: for reliable scanning, entire files must be scanned.

If undesirable, this rule can be disabled. This is not recommended as it might jeopardize scanning reliability. However, there is a more secure way to limit this behavior: create a rule which will allow unlimited connections to a particular FTP server. The rule will take effect only if it is placed before the *Resume* rule.

For details on antivirus scan of FTP protocol, refer to chapter 11.3.

FTP Rules Definition

To create a new rule, select a rule after which the new rule will be added, and click *Add*. You can later use the arrow buttons to reorder the rule list.

Checking the box next to the rule can be used to disable the rule. Rules can be disabled temporarily so that it is not necessary to remove rules and create identical ones later.

Note: FTP traffic which does not match any FTP rule is allowed (any traffic permitted by default). To allow accessing only a specific group of FTP servers and block access to other web pages, a rule denying access to all FTP servers must be placed at the end of the rule list.

FTP rule dialog:

Open the *General* tab to set general rules and actions to be taken.

Description
Description of the rule (information for the administrator).

If user accessing the FTP server is
Select which users this rule will be applied on:

- *any user* — the rule will be applied on all users (regardless whether authenticated on the firewall or not).
- *any user authenticated on the firewall* — applied on all authenticated users.
- *selected user(s)* — applied on selected users or/and user groups.
  Click on the *Set* button to select users or groups (hold the *Ctrl* and the *Shift* keys to select more that one user /group at once).

Note: Rules designed for selected users (or all authenticated users) are irrelevant unless combined with a rule that denies access of non-authenticated users.

And the FTP server is
Specify FTP servers on which this rule will be applied:

- *any server* —any FTP server
- *server* — IP address of DNS name of a particular FTP server.
  If an FTP server is defined through a DNS name, *WinRoute* will automatically perform IP address resolution from DNS. The IP address will be resolved immediately when settings are confirmed by the *OK* button (for all rules where the FTP server was defined by a DNS name).

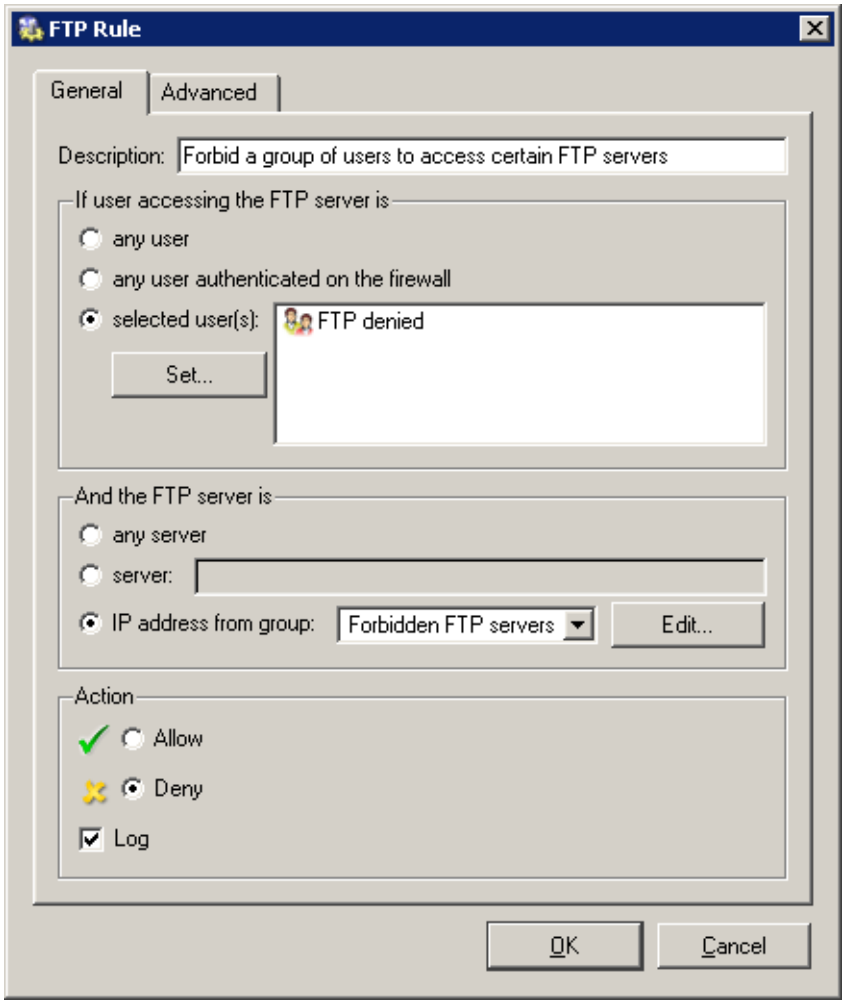


Figure 10.15 FTP Rule — basic parameters

Warning: Rules are disabled unless a corresponding IP address is found!

- *IP address from group* — selection of IP addresses of FTP servers that will be either denied or allowed.
  Click on the *Edit* button to edit IP groups (for details see chapter 12.1).

Action

Select an action that will be taken when requirements for users and the FTP server are met:

- *Allow* — *WinRoute* allows connection to selected FTP servers under conditions set in the *Advanced* tab— see below).
- *Deny* — *WinRoute* will block certain FTP commands or FTP connections (according to the settings within the *Advanced* tab).

Check the *Log* option to log all FTP connections meeting this rule in the *Filter* log

(see chapter 20.9).

Go to the *Advanced* tab to define other conditions that must be met for the rule to be applied and to set advanced options for FTP communication.

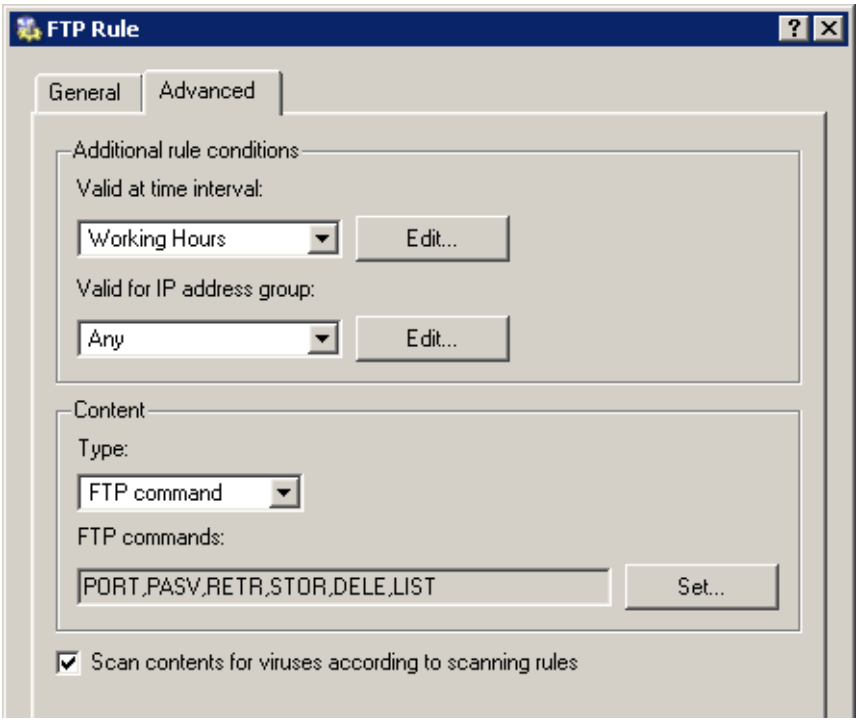


Figure 10.16 FTP Rule — advanced settings

Valid at time interval

Selection of the time interval during which the rule will be valid (apart from this interval the rule will be ignored). Use the *Edit* button to edit time intervals (for details see chapter 12.2).

Valid for IP address group

Selection of IP address group on which the rule will be applied. Client (source) addresses are considered. Use the *Any* option to make the rule independent of clients.

Click on the *Edit* button to edit IP groups (for details see chapter 12.1).

Content

Advanced options for FTP traffic content.

Use the *Type* option to set a filtering method:

- *Download*, *Upload*, *Download / Upload* — transport of files in one or both directions.

If any of these options is chosen, you can specify names of files on which the rule will be applied using the *File name* entry. Wildcard matching can be used to specify a file name (i.e. `*.exe` for executables).

- *FTP command* — selection of commands for the FTP server on which the rule will be applied
- *Any* — denies all traffic (any connection or command use)

Scan content for viruses according to scanning rules

Use this option to enable/disable scanning for viruses for FTP traffic which meet this rule.

This option is available only for allowing rules — it is meaningless to apply antivirus check to denied traffic.

Chapter 11

Antivirus control

WinRoute provides antivirus check of objects (files) transmitted by HTTP, FTP, SMTP and POP3 protocols. In case of HTTP and FTP protocols, the *WinRoute* administrator can specify which types of objects will be scanned.

WinRoute is also distributed in a special version which includes integrated *McAfee* antivirus. Besides the integrated antivirus, *WinRoute* supports several antivirus programs developed by various companies, such as Eset Software, Grisoft, F-Secure, etc.). Antivirus licenses must meet the license policy of a corresponding company (usually, the license is limited by the same or higher number of users as *WinRoute* is licensed for, or a server license).

Since *6.2.0*, *WinRoute* enables to combine the integrated *McAfee* antivirus with a supported external antivirus. In such a case, transferred files are checked by both antiviruses (so called dual antivirus control). This feature reduces the risk of letting in a harmful file.

However, using of two antiviruses at a time also decreases the speed of firewall's performance. It is therefore highly recommended to consider thoroughly which method of antivirus check should be used and to which protocols it should be applied and, if possible and desired, to try the configuration in the trial version of *WinRoute* before purchasing a license.

Notes:

1. However, supported external antiviruses as well as versions and license policy of individual programs may change as the time flows. For up-to-date information please refer to (`http://www.kerio.com/kwf`).

2. External *McAfee Anti-Virus* programs are not supported by *WinRoute*.

11.1 Conditions and limitations of antivirus scan

Antivirus check of objects transferred by a particular protocol can be applied only to traffic where a corresponding protocol inspector which supports the antivirus is used

(see chapter 12.3). This implies that the antivirus check is limited by the following factors:

- Antivirus check cannot be used if the traffic is transferred by a secured channel (SSL/TLS). In such a case, it is not possible to decipher traffic and separate transferred objects.

- Within email antivirus scanning (SMTP and POP3 protocols), the firewall only removes infected attachments — it is not possible to drop entire email messages. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Check of outgoing traffic causes problems with temporarily undeliverable email.

  For details, see chapter 11.4.

- Object transferred by other than HTTP, FTP, SMTP and POP3 protocols cannot be checked by an antivirus.

- If a substandard port is used for the traffic, corresponding protocol inspector will not be applied automatically. In that case, simply define a traffic rule which will allow this traffic using a corresponding protocol inspector (for details, see chapter 6.3).

  Example: You want to perform antivirus checks of the HTTP protocol at port 8080.

  1. Define the *HTTP 8080* service (TCP protocol, port 8080).

  2. Create a traffic rule which will allow this service applying a corresponding protocol inspector.

Name	Source	Destination	Service	Action	Protocol Inspector
HTTP 8080 with inspection	Any	Any	HTTP 8080	✓	HTTP

Figure 11.1 Traffic rule for HTTP protocol inspection at non-standard ports

  Add the new rule before the rule allowing access to any service in the Internet (if such a rule exists). If the NAT (source address translation) technology is used for Internet connection, address translation must be set for this rule as well.

  Note: A corresponding protocol inspector can be also specified within the service definition, or both definition methods can be used. Both methods yield the same result, however, the corresponding traffic rule is more transparent when the protocol inspector is defined in it.

11.2 How to choose and setup antiviruses

To select antiviruses and set their parameters, open the *Antivirus* tab in *Configuration* → *Content Filtering* → *Antivirus*. Ob this tab, you can select the integrated *McAfee* module, an external antivirus, or both.

If both antiviruses are used, each transferred object (downloaded file, an email attachment, etc.) will be first checked by the integrated *McAfee* antivirus module and then by the other antivirus (a selected external antivirus).

Integrated McAfee

To enable the integrated *McAfee* antivirus, enable *Use integrated McAfee antivirus engine* in the *Antivirus* tab. This option is not available unless the license key for *WinRoute* includes a license for the *McAfee* antivirus or in trial versions. For detailed information about the licensing policy, read chapter 44.

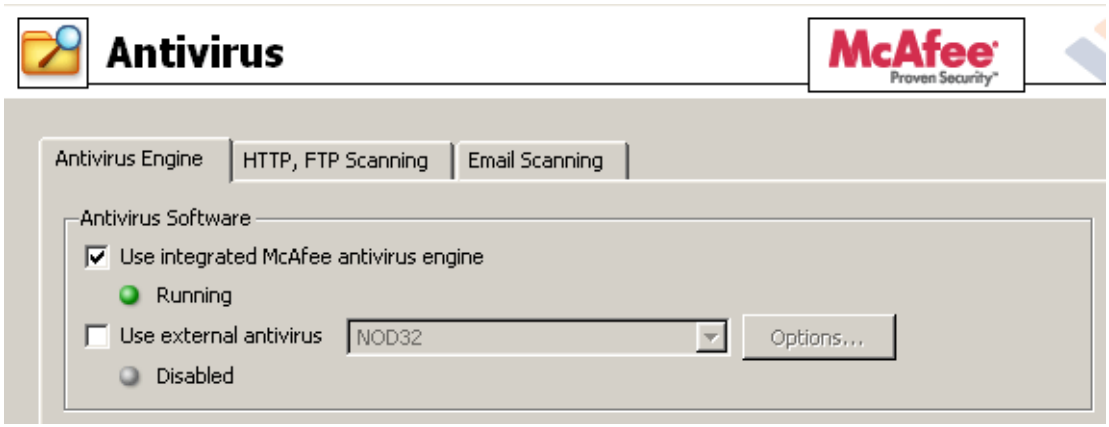


Figure 11.2 Antivirus selection (integrated antivirus)

Use the *Integrated antivirus engine* section in the *Antivirus* tab to set update parameters for *McAfee*.

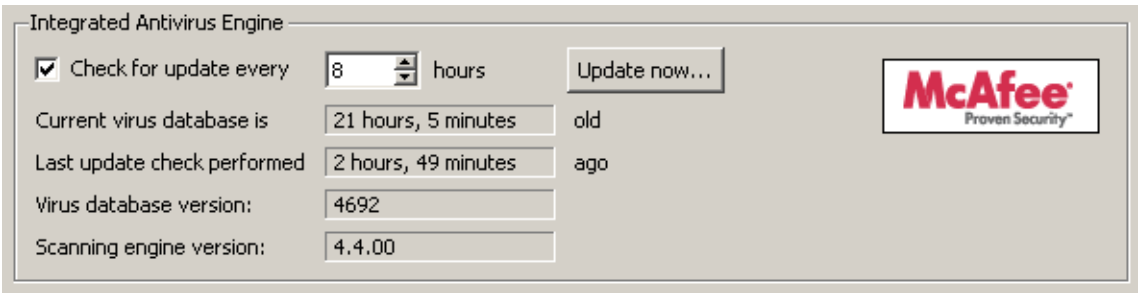


Figure 11.3 Scheduling McAfee updates

Check for update every ... hours

Time interval of checks for new updates of the virus database and the antivirus engine (in hours).

If any new update is available, it will be downloaded automatically by *WinRoute*.

If the update attempt fails (i.e. the server is not available), detailed information about the attempt will be logged into the *Error* log (refer to chapter 20.8).

Each download (update) attempt sets the *Last update check performed* value to zero.

Warning: To make the antivirus control as mighty as possible, it is necessary that the antivirus module is always equipped by the most recent version of the virus database. Therefore, it is recommended to keep automatic updates running and not to set too long intervals between update checks (update checks should be performed at least twice a day).

Current virus database is ...

Information regarding the age of the current database.

Note: If the value is too high, this may indicate that updates of the database have failed several times. In such cases, we recommend you to perform a manual update check by the *Update now* button and view the *Error* log.

Last update check performed ... ago

Time that has passed since the last update check.

Virus database version

Database version that is currently used.

Scanning engine version

McAfee scanning engine version used by *WinRoute*.

Update now

Use this button for immediate update of the virus database and of the scanning engine.

After you run the update check using the *Update now...* button, an informational window displaying the update check process will be opened. You can use the *OK* button to close it — it is not necessary to wait until the update is finished.

If updated successfully, the version number of the new virus database or/and the new antivirus version(s), as well as information regarding the age of the current virus database will be displayed. If the update check fails (i.e. the server is not available), an error will be reported and detailed information about the update attempt will be logged into the *Error* log.

Each download (update) attempt sets the *Last update check performed* value to zero.

External antivirus

For external antivirus, enable the *Use external antivirus* option in the *Antivirus* tab and select an antivirus to be employed from the combo box. This menu provides all external antivirus programs supported in *WinRoute* by special *plugins*.

Warning: External antivirus must be installed before it is set, otherwise it is not available in the combo box. It is recommended to stop the *WinRoute Firewall Engine* service before an antivirus installation.

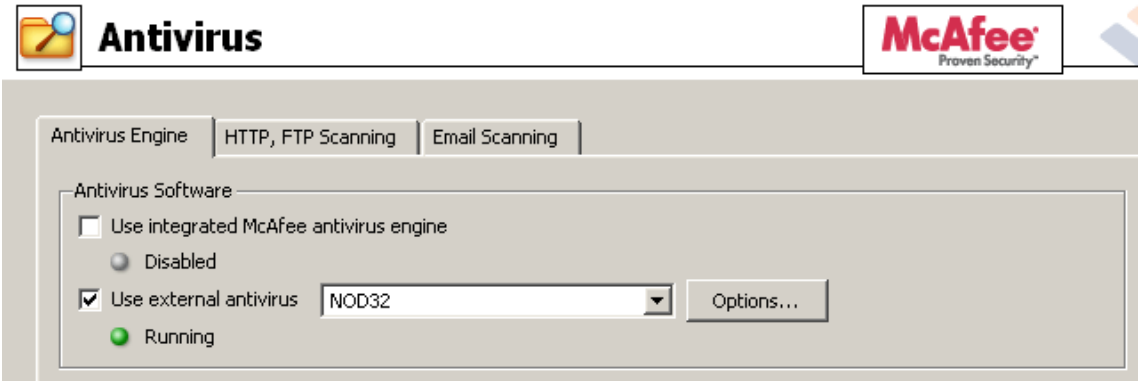


Figure 11.4 Antivirus selection (external antivirus)

Use the *Options* button to set advanced parameters for the selected antivirus. Dialogs for individual antiviruses differ (some antivirus programs may not require any additional settings). For detailed information about installation and configuration of individual antivirus programs, refer to `http://www.kerio.com/kwf`.

Click *Apply* to test the selected antivirus. If the test is passed successfully, the antivirus will be used from the moment on. If not, an error is reported and no antivirus will be set. Detailed information about the failure will be reported in the *Error* log (see chapter 20.8).

Antivirus settings

Check items in the *Settings* section of the *Antivirus* tab to enable antivirus check for individual application protocols. By default, antivirus check is enabled for all supported modules.

In *Settings*, maximum size of files to be scanned for viruses at the firewall can be set. Scanning of large files are demanding for time, the processor and free disk space, which might affect the firewall's functionality dramatically. It might happen that the connection over which the file is transferred is interrupted when the time limit is exceeded.

The optimal value of the file size depends on particular conditions (the server's performance, load on the network, type of the data transmitted, antivirus type, etc.). *Caution!*

We strongly discourage administrators from changing the default value for file size limit. In any case, do not set the value to more than 4 MB.

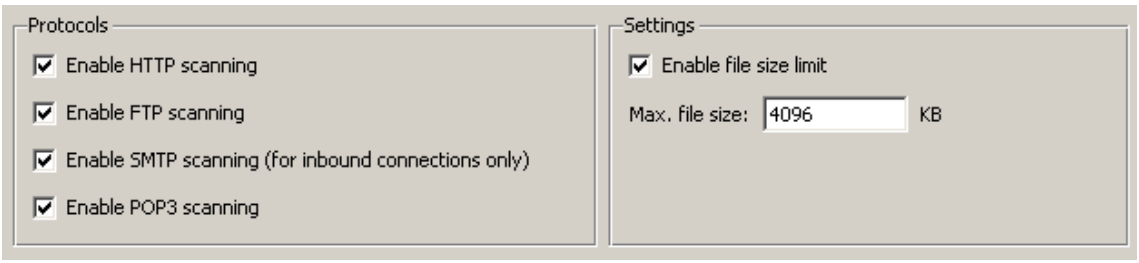


Figure 11.5 Selecting application protocols to be scanned and setting file size limits

Parameters for HTTP and FTP scanning can be set in the *HTTP and FTP scanning* (refer to chapter 11.3), while SMTP and POP3 scanning can be configured in the *Email scanning* tab (see chapter 11.4).

Warning:

1. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Checks of outgoing SMTP traffic (from the local network to the Internet) might cause problems with temporarily undeliverable email — for example in cases where the destination SMTP server uses so called *greylisting*.

   To perform smooth checks of outgoing traffic, define a corresponding traffic rule using the SMTP protocol inspector. Such rule may be useful for example if clients in the local network send their email via an SMTP server located in the Internet. Checking of outgoing SMTP traffic is not apt for local SMTP servers sending email to the Internet.

   An example of a traffic rule for checking of outgoing SMTP traffic is shown at figure 11.6.

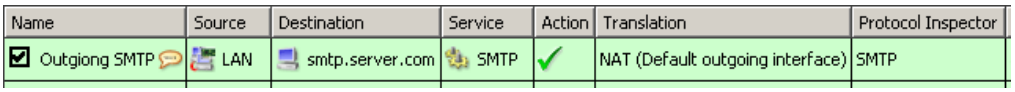


Figure 11.6 An example of a traffic rule for outgoing SMTP traffic check

2. Substandard extensions of the SMTP protocol can be used in case of communication of two *Microsoft Exchange* mailservers. Under certain conditions, email messages are transmitted in form of binary data. In such a case, *WinRoute* cannot perform antivirus check of individual attachments.

   In such cases, it is recommended to use an antivirus which supports *Microsoft Exchange* and not to perform antivirus check of SMTP traffic of a particular server

in *WinRoute*. To achieve this, disable antivirus check for SMTP protocol or define a corresponding traffic rule where no protocol inspector will be applied (see chapter 23.4).

11.3 HTTP and FTP scanning

As for HTTP and FTP traffic, objects (files) of selected types are scanned.

The file just transmitted is saved in a temporary file on the local disk of the firewall. *WinRoute* caches the last part of the transmitted file (segment of the data transferred) and performs an antivirus scan of the temporary file. If a virus is detected in the file, the last segment of the data is dropped. This means that the client receives an incomplete (damaged) file which cannot be executed so that the virus cannot be activated. If no virus is found, *WinRoute* sends the client the rest of the file and the transmission is completed successfully.

Optionally, a warning message informing about a virus detected can be sent to the user who tried to download the file (see the *Notify user by email* option).

Warning:

1. The purpose of the antivirus check is only to detect infected files, it is not possible to heal them!

2. If the antivirus check is disabled in HTTP and FTP filtering rules, objects and files matching corresponding rules are not checked. For details, refer to chapters 10.2 and 10.6).

3. Full functionality of HTTP scanning is not guaranteed if any non-standard extensions to web browsers (e.g. download managers, accelerators, etc.) are used!

To set parameters of HTTP and FTP antivirus check, open the *HTTP, FTP scanning* tab in *Configuration → Content Filtering → Antivirus*.

Use the *If a virus is found...* entry to specify actions to be taken whenever a virus is detected in a transmitted file:

- *Move the file to quarantine* — the file will be saved in a special directory on the *WinRoute* host. *WinRoute* administrators can later try to heal the file using an antivirus program and if the file is recovered successfully, the administrator can provide it to the user who attempted to download it.

  The `quarantine` subdirectory under the *WinRoute* directory is used for the quarantine

  (the typical path is `C:\Program Files\Kerio\WinRoute Firewall\quarantine`).

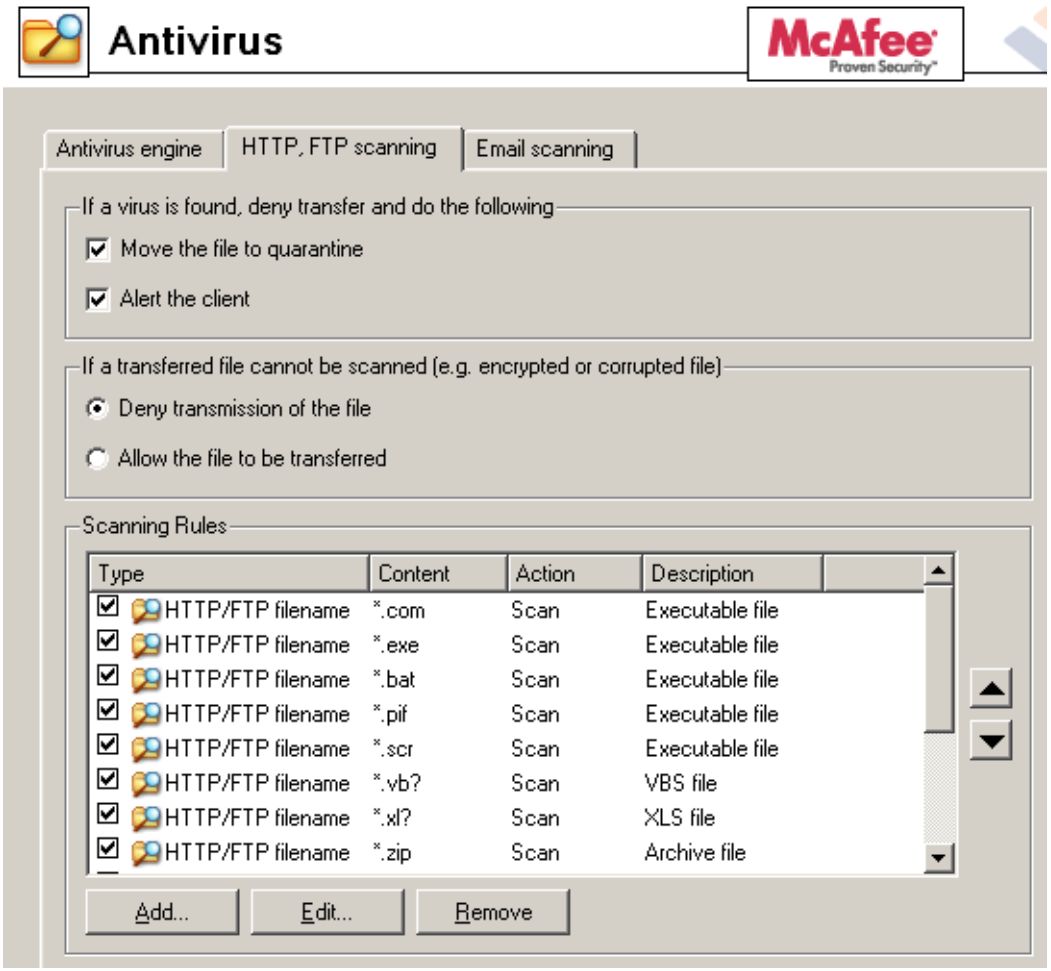


Figure 11.7 Settings for HTTP and FTP scanning

Infected files (files which are suspected of being infected) are saved into this directory with names which are generated automatically. Name of each file includes information about protocol, date, time and connection number used for the transmission.

Warning: When handling files in the `quarantine` directory, please consider carefully each action you take, otherwise a virus might be activated and the *WinRoute* host could be attacked by the virus!

- *Alert the client* — *WinRoute* alerts the user who attempted to download the file by an email message warning that a virus was detected and download was stopped for security reasons.

  WinRoute sends alert messages under the following circumstances: The user is authenticated and connected to the firewall, a valid email address is set in a corre-

sponding user account (see chapter 13.1) and the SMTP server used for mail sending is configured correctly (refer to chapter 16.4).

Note: Regardless of the fact whether the *Alert the client* option is used, alerts can be sent to specified addresses (e.g. addresses of network administrators) whenever a virus is detected. For details, refer to chapter 17.3.

In the *If the transferred file cannot be scanned* section, actions to be taken when the antivirus check cannot be applied to a file (e.g. the file is compressed and password-protected, damaged, etc.):

- *Deny transmission of the file* — *WinRoute* will consider these files as infected and deny their transmission.

  HINT: It is recommended to combine this option with the *Move the file to quarantine* function — the *WinRoute* administrator can extract the file and perform manual antivirus check if a user asks him/her

- *Allow the file to be transferred* — *WinRoute* will treat compressed password-protected files and damaged files as trustful (not infected).

  Generally, use of this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files and the antivirus is installed on the workstations.

HTTP and FTP scanning rules

These rules specify when antivirus check will be applied. By default (if no rule is defined), all objects transmitted by HTTP and FTP are scanned.

Note: WinRoute contains a set of predefined rules for HTTP and FTP scanning. By default, all executable files as well as all *Microsoft Office* files are scanned. The *WinRoute* administrator can change the default configuration.

Scanning rules are ordered in a list and processed from the top. Arrow buttons on the right can be used to change the order. When a rule which matches the object is found, the appropriate action is taken and rule processing is stopped.

New rules can be created in the dialog box which is opened after clicking the *Add* button.

Description
Description of the rule (for reference of the *WinRoute* administrator only)

Condition
Condition of the rule:

- *HTTP/FTP filename*

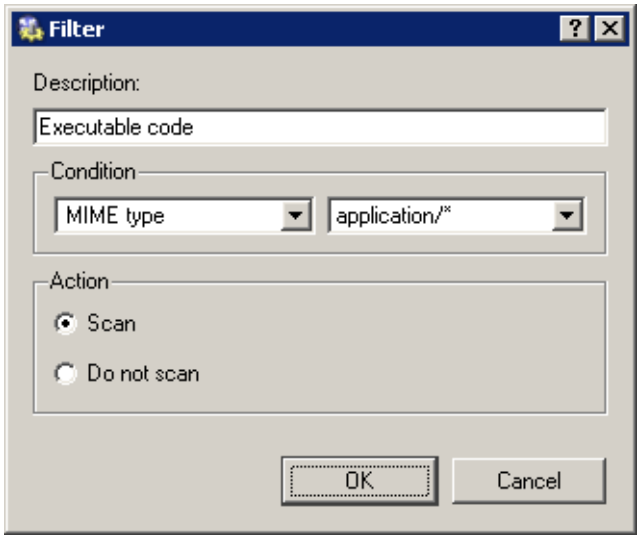


Figure 11.8 Definition of an HTTP/FTP scanning rule

— this option filters out certain filenames (not entire URLs) transmitted by FTP or HTTP (e.g. `*.exe`, `*.zip`, etc.).
If only an asterisk is used for the specification, the rule will apply to any file transmitted by HTTP or FTP.

The other two conditions can be applied only to HTTP:

- *MIME type*
  — MIME types can be specified either by complete expressions (e.g. `image/jpeg`) or using a wildcard matching (e.g. `application/*`).
- *URL* — URL of the object (e.g. `www.kerio.com/img/logo.gif`), a string specified by a wildcard matching (e.g. `*.exe`) or a server name (e.g. `www.kerio.com`). Server names represent any URL at a corresponding server (`www.kerio.com/*`).

If a MIME type or a URL is specified only by an asterisk, the rule will apply to any HTTP object.

Action

Settings in this section define whether or not the object will be scanned.
If the *Do not scan* alternative is selected, antivirus control will not apply to transmission of this object.

The new rule will be added after the rule which had been selected before *Add* was clicked. You can use the arrow buttons on the right to move the rule within the list.

Checking the box next to the rule can be used to disable the rule. Rules can be disabled temporarily so that it is not necessary to remove rules and create identical ones later.

Note: If the object does not match with any rule, it will be scanned automatically. If only selected object types are to be scanned, a rule disabling scanning of any URL or MIME

type must be added to the end of the list (the *Skip all other files* rule is predefined for this purpose).

11.4 Email scanning

SMTP and POP3 protocols scanning settings are defined through this tab. If scanning is enabled for at least one of these protocols, all attachments of transmitted messages are scanned.

Individual attachments of transmitted messages are saved in a temporary directory on the local disk. When downloaded completely, the files are scanned for viruses. If no virus is found, the attachment is added to the message again. If a virus is detected, the attachment is replaced by a notice informing about the virus found.

Note: Warning messages can also be sent to specified email addresses (e.g. to network administrators) when a virus is detected. For details, refer to chapter 17.3.

Warning:

1. Antivirus control within WinRoute can only detect and block infected attachments. Attached files cannot be healed by this control!

2. Within antivirus scanning, it is possible to remove only infected attachments, entire email messages cannot be dropped. This is caused by the fact that the firewall cannot handle email messages like mailservers do. It only maintains network traffic coming through. In most cases, removal of an entire message would lead to a failure in communication with the server and the client might attempt to send/download the message once again. Thus, one infected message might block sending/reception of any other (legal) mail.

3. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Checks of outgoing SMTP traffic (i.e. from the local network to the Internet) might cause problems with temporarily undeliverable email (for example in cases where the destination SMTP server uses so called *greylisting*).

   To check also outgoing traffic (e.g. when local clients connect to an SMTP server without the local network), define a corresponding traffic rule using the SMTP protocol inspector. For details, see chapter 11.2.

Advanced parameters and actions that will be taken when a virus is detected can be set in the *Email scanning* tab.

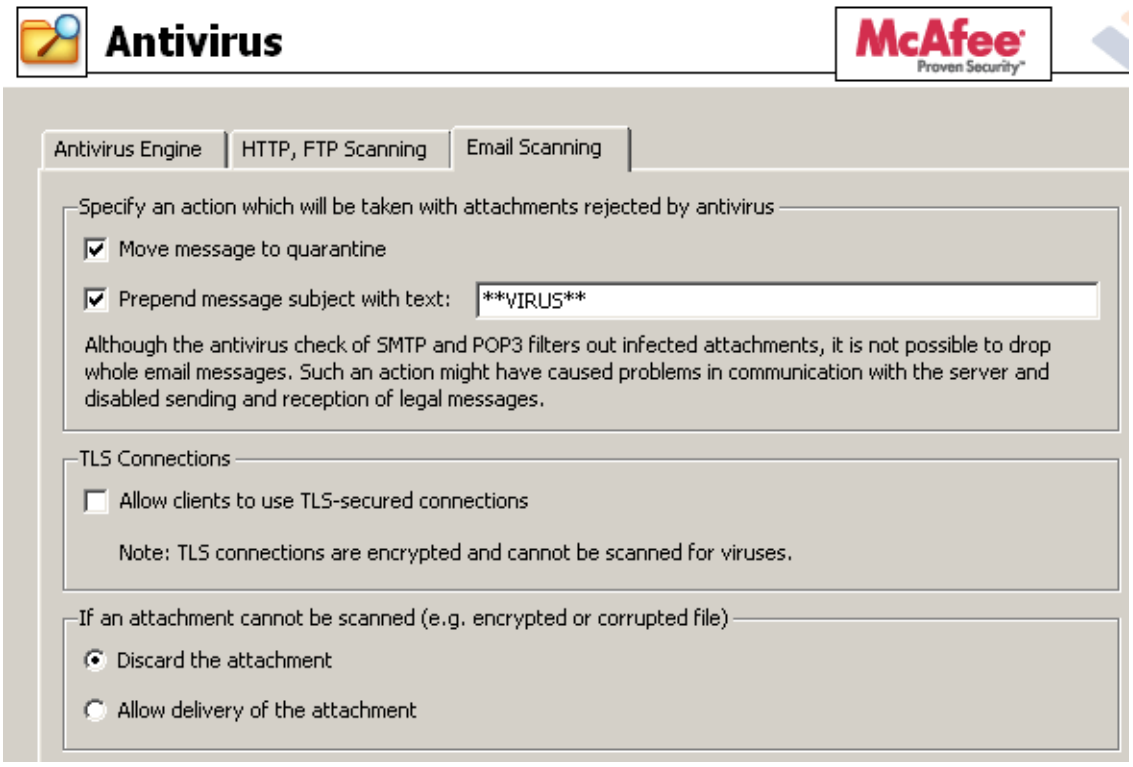

Antivirus
McAfee
Proven Security
Antivirus Engine
HTTP, FTP Scanning
Email Scanning
Specify an action which will be taken with attachments rejected by antivirus
Move message to quarantine
Prepend message subject with text:
VIRUS
Although the antivirus check of SMTP and POP3 filters out infected attachments, it is not possible to drop whole email messages. Such an action might have caused problems in communication with the server and disabled sending and reception of legal messages.
TLS Connections
Allow clients to use TLS-secured connections
Note: TLS connections are encrypted and cannot be scanned for viruses.
If an attachment cannot be scanned (e.g. encrypted or corrupted file)
Discard the attachment
Allow delivery of the attachment

Figure 11.9 Settings for SMTP and POP3 scanning

In the *Specify an action which will be taken with attachments...* section, the following actions can be set for messages considered by the antivirus as infected:

- *Move message to quarantine* — untrustworthy messages will be moved to a special directory on the *WinRoute* host. The *WinRoute* administrator can try to heal infected files and later send them to their original addressees.

  The `quarantine` subdirectory under the *WinRoute* directory is used for the quarantine

  (the typical path is `C:\Program Files\Kerio\WinRoute Firewall\quarantine`). Messages with untrustworthy attachments are saved to this directory under names which are generated automatically by *WinRoute*. Each filename includes information about protocol, date, time and the connection number used for transmission of the message.

- *Prepend subject message with text* — use this option to specify a text to be attached before the subject of each email message where at least one infected attachment is found. This text informs the recipient of the message and it can be also used for automatic message filtering.

Note: Regardless of what action is set to be taken, the attachment is always removed and a warning message is attached instead.

Use the *TLS connections* section to set firewall behavior for cases where both mail client and the server support TLS-secured SMTP or POP3 traffic.

In case that TLS protocol is used, unencrypted connection is established first. Then, client and server agree on switching to the secure mode (encrypted connection). If the client or the server does not support TLS, encrypted connection is not used and the traffic is performed in a non-secured way.

If the connection is encrypted, firewall cannot analyze it and perform antivirus check for transmitted messages. *WinRoute* administrator can select one of the following alternatives:

- Enable TLS. This alternative is suitable for such cases where protection from wiretapping is prior to antivirus check of email.

  HINT: In such cases, it is recommended to install an antivirus engine at individual hosts that would perform local antivirus check.

- Disable TLS. Secure mode will not be available. Clients will automatically assume that the server does not support TLS and messages will be transmitted through an unencrypted connection. Firewall will perform antivirus check for all transmitted mail.

The *If an attachment cannot be scanned* section defines actions to be taken if one or multiple files attached to a message cannot be scanned for any reason (e.g. password-protected archives, damaged files, etc.):

- *Reject the attachment* — *WinRoute* reacts in the same way as when a virus was detected (including all the actions described above).

- *Allow delivery of the attachment* — *WinRoute* behaves as if password-protected or damaged files were not infected.

  Generally, this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files (typically password-protected archives) and the antivirus is installed on the workstations.

Chapter 12

Definitions

12.1 IP Address Groups

IP groups are used for simple access to certain services (e.g. *WinRoute's* remote administration, Web server located in the local network available from the Internet, etc.). When setting access rights a group name is used. The group itself can contain any combination of computers (IP addresses), IP address ranges, subnets or other groups.

Creating and Editing IP Address Groups

You can define IP address groups in the *Configuration* → *Definitions* → *IP Address Groups* section.

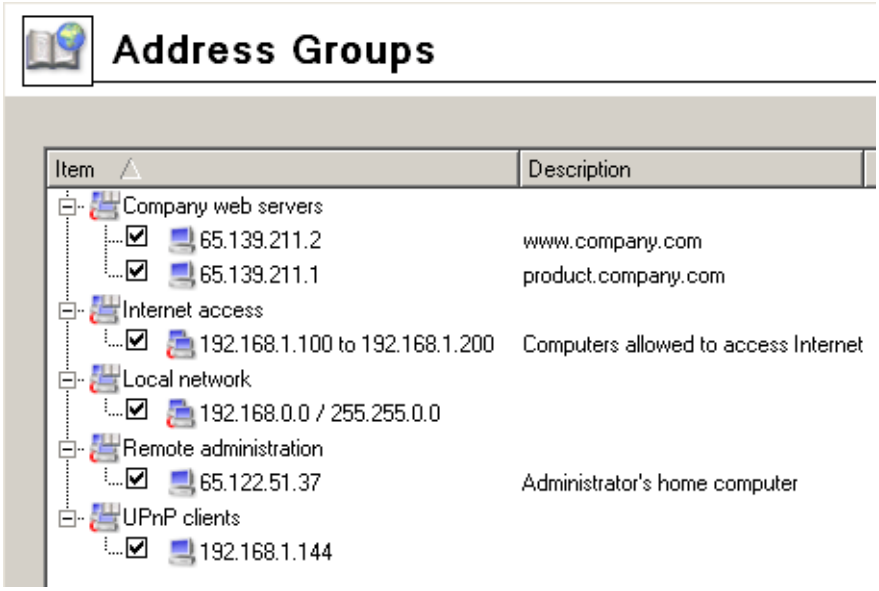


Figure 12.1 WinRoute's IP groups

Click on *Add* to add a new group (or an item to an existing group) and use *Edit* or *Delete* to edit or delete a selected group or item.

The following dialog window is displayed when you click on the *Add* button:

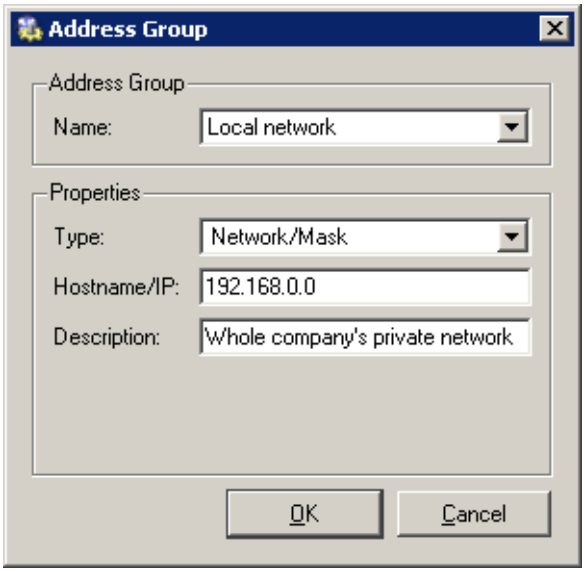


Figure 12.2 IP group definition

Name
The name of the group. Add a new name to create a new group. Insert the group name to add a new item to an existent group.

Type
Type of the new item:

- *Host* (IP address or DNS name of a particular host)
- *Network / Mask* (subnet with a corresponding mask)
- *Network / Range* (IP range)
- *Address group* (another group of IP addresses — groups can be cascaded)

IP address, Mask...
Parameters of the new item (related to the selected type).

Description
Commentary for the IP address group. This helps guide the administrator.

Note: Each IP group must include at least one item. Groups with no item will be removed automatically.

12.2 Time Intervals

Time ranges in *WinRoute* are closely related to traffic policy rules (see chapter 6). *WinRoute* allows the administrator to set a time period where each rule will be applied. These time ranges are actually groups that can consist of any number of various intervals and single actions.

Using time ranges you can also set dial-up parameters — see chapter 5.1.

To define time ranges go to *Configuration* → *Definitions* → *Time Ranges*.

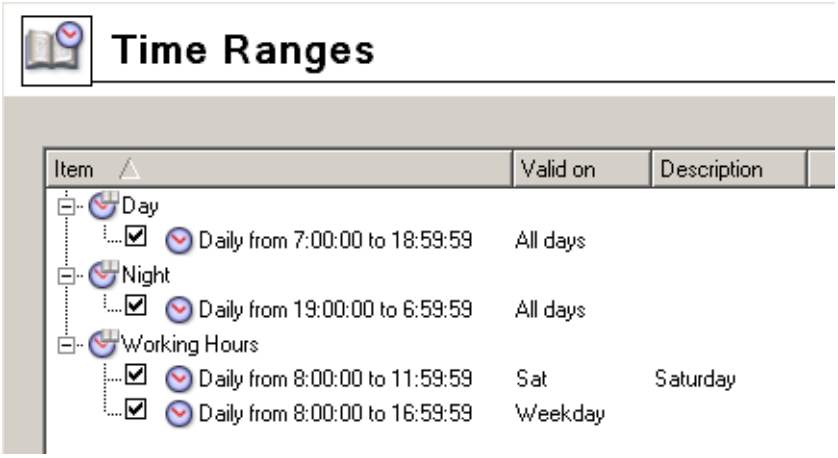


Figure 12.3 WinRoute's time intervals

Time range types

When defining a time interval three types of time ranges (subintervals) can be used:

Absolute
: The time interval is defined with the initial and expiration date and it is not repeated

Weekly
: This interval is repeated weekly (according to the day schedule)

Daily
: It is repeated daily (according to the hour schedule)

Defining Time Intervals

Time ranges can created, edited and removed in *Configuration* → *Definitions* → *Time Ranges*.

Clicking on the *Add* button will display the following dialog window:

Name
: Name (identification) of the time interval. Insert a new name to create a new time range. Insert the name of an existent time range to add a new item to this range.

Description
: Time ranges description, for the administrator only

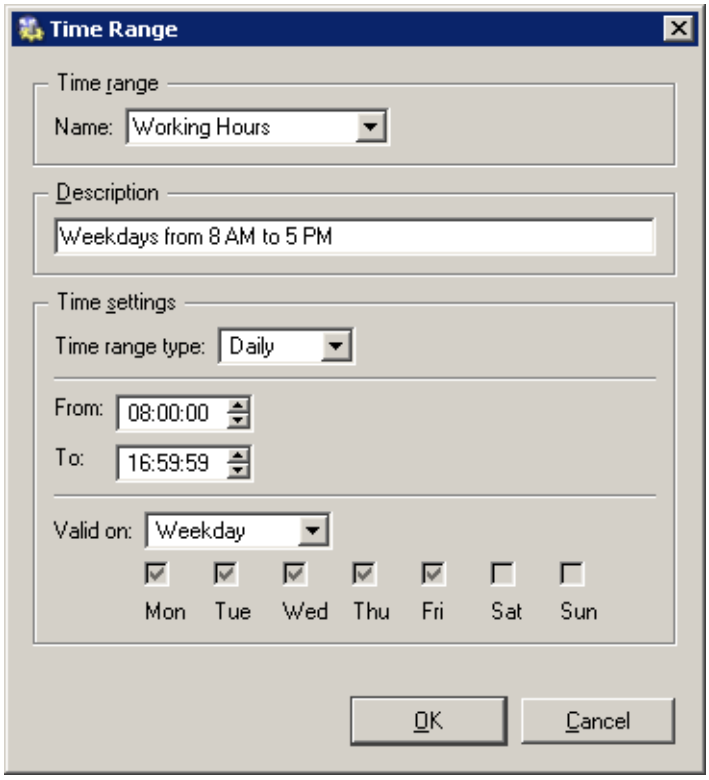


Figure 12.4 Time range definition

Time Interval Type

Time range type: *Daily*, *Weekly* or *Absolute*. The last type refers to the user defined initial and terminal date.

From, To

The beginning and the end of the time range. Beginning and end hours, days or dates can be defined according to the selected time range type

Valid at days

Defines days when the interval will be valid. You can either select particular weekdays (*Selected days*) or use one of the predefined options (*All Days*, *Weekday* — from Monday to Friday, *Weekend* — Saturday and Sunday).

Notes:

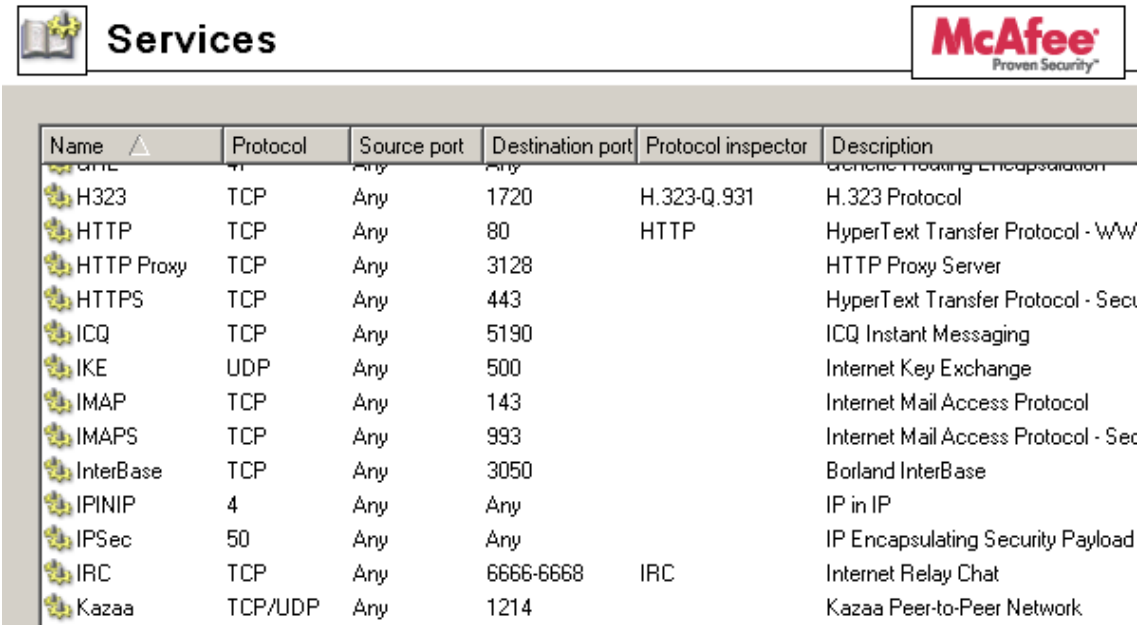
1. each time range must contain at least one item. Time ranges with no item will be removed automatically.

2. Time intervals cannot be cascaded.

12.3 Services

WinRoute services enable the administrator to define communication rules easily (by permitting or denying access to the Internet from the local network or by allowing access to the local network from the Internet). Services are defined by a communication protocol and by a port number (e.g. the *HTTP* service uses the TCP protocol with the port number 80). You can also match so-called protocol inspector with certain service types (for details see below).

Services can be defined in *Configurations* → *Definitions* → *Services*. Some standard services, such as HTTP, FTP, DNS etc., are already predefined in the default *WinRoute* installation.



Name	Protocol	Source port	Destination port	Protocol inspector	Description
H323	TCP	Any	1720	H.323-Q.931	H.323 Protocol
HTTP	TCP	Any	80	HTTP	HyperText Transfer Protocol - WW
HTTP Proxy	TCP	Any	3128		HTTP Proxy Server
HTTPS	TCP	Any	443		HyperText Transfer Protocol - Secu
ICQ	TCP	Any	5190		ICQ Instant Messaging
IKE	UDP	Any	500		Internet Key Exchange
IMAP	TCP	Any	143		Internet Mail Access Protocol
IMAPS	TCP	Any	993		Internet Mail Access Protocol - Sec
InterBase	TCP	Any	3050		Borland InterBase
IPINIP	4	Any	Any		IP in IP
IPSec	50	Any	Any		IP Encapsulating Security Payload
IRC	TCP	Any	6666-6668	IRC	Internet Relay Chat
Kazaa	TCP/UDP	Any	1214		Kazaa Peer-to-Peer Network

Figure 12.5 WinRoute's network services

Clicking on the *Add* or the *Edit* button will open a dialog for service definition.

Name

Service identification within *WinRoute*. It is strongly recommended to use a concise name to keep the program easy to follow.

Description

Comments for the service defined. It is strongly recommended describing each definition, especially with non-standard services so that there will be minimum confusion when referring to the service at a later time.

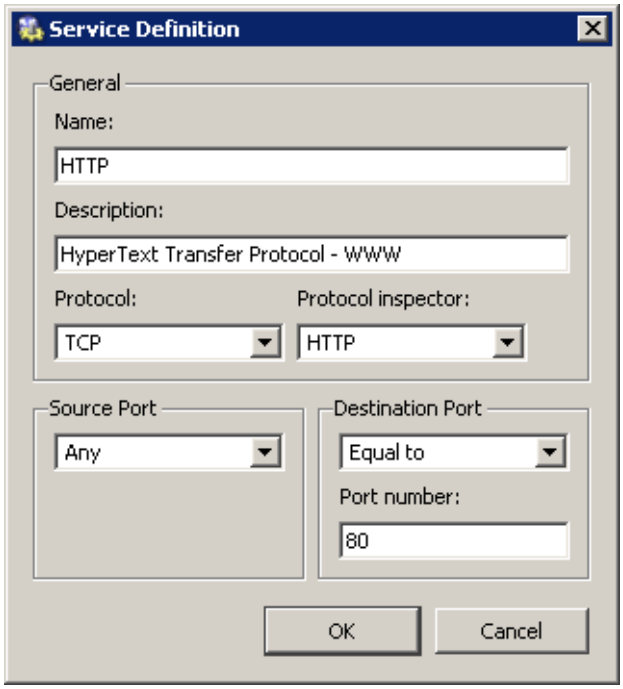


Figure 12.6 Network service definition

Protocol

The communication protocol used by the service.

Most standard services uses the *TCP* or the *UDP* protocol, or both when they can be defined as one service with the *TCP/UDP* option. Other options available are *ICMP* and *other*.

The *other* options allows protocol specification by the number in the IP packet header. Any protocol carried in IP (e.g. GRE — protocol number is 47) can be defined this way.

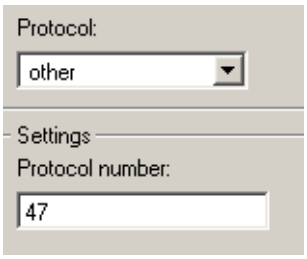


Figure 12.7 Setting a protocol in service definition

Protocol inspector

WinRoute protocol inspector (see below) that will be used for this service.

Warning: Each inspector should be used for the appropriate service only. Functionality of the service might be affected by using an inappropriate inspector.

Source Port and Destination Port

If the TCP or UDP communication protocol is used, the service is defined with its port number. In case of standard client-server types, a server is listening for connections on a particular port (the number relates to the service), whereas clients do not know their port in advance (port are assigned to clients during connection attempts). This means that source ports are usually not specified, while destination ports are usually known in case of standard services.

Note: Specification of the source port may be important, for example during the definition of communication filter rules. For details, refer to chapter 6.3.

Source and destination ports can be specified as:

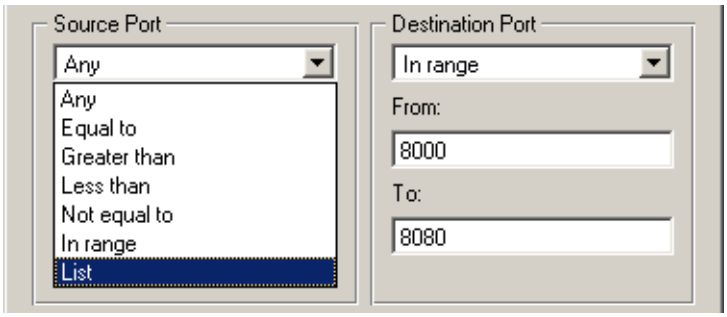


Figure 12.8 Service definition — source and destination port setting

- *Any* — all the ports available (`1-65535`)
- *Equal to* —a particular port (e.g.`80`)
- *Greater than*, *Less than* — all ports with a number that is either greater or less than the number defined
- *Not equal to* — all ports that are not equal to the one defined
- *In range* — all ports that fit to the range defined (including the initial and the terminal ones)
- *List* — list of the ports divided by comas (e.g. `80,8000,8080`)

Protocol Inspectors

WinRoute includes special plug-ins that monitor all traffic using application protocols, such as HTTP, FTP or others. The modules can be used to modify (filter) the communication or adapt the firewall's behavior according to the protocol type. Benefits of protocol inspectors can be better understood through the two following examples:

1. *HTTP protocol inspector* monitors traffic between clients (browsers) and Web servers. It can be used to block connections to particular pages or downloads of particular objects (i.e. images, pop-ups, etc.).

2. With active FTP, the server opens a data connection to the client. Under certain conditions this connection type cannot be made through firewalls, therefore FTP

can only be used in passive mode. The *FTP protocol inspector* distinguishes that the FTP is active, opens the appropriate port and redirects the connection to the appropriate client in the local network. Due to this fact, users in the local network are not limited by the firewall and they can use both FTP modes (active/passive).

The protocol inspector is enabled if it is set in the service definition and if the corresponding traffic is allowed. Each protocol inspector applies to a specific protocol and service. In the default *WinRoute* configuration, all available protocol inspectors are used in definitions of corresponding services (so they will be applied to corresponding traffic automatically), except protocol inspectors for *SIP*and *H.323* (*SIP* and *H.323* are complex protocols and protocol inspectors may work incorrectly in some configurations).

To apply a protocol inspector explicitly to another traffic, it is necessary to define a new service where this inspector will be used or to set the protocol inspector directly in the corresponding traffic rule.

Example: You want to perform inspection of the HTTP protocol at port 8080. Define a new service: TCP protocol, port 8080, HTTP protocol inspector. This ensures that *HTTP* protocol inspector will be automatically applied to any *TCP* traffic at port 8080 and passing through *WinRoute*.

Notes:

1. Generally, protocol inspectors cannot be applied to secured traffic (SSL/TLS). In this case, *WinRoute* "percieves" the traffic as binary data only. This implies that such traffic cannot be deciphered.

2. Under certain circumstances, appliance of a protocol inspector is not desirable. Therefore, it is possible to disable a corresponding inspector temporarily. For details, refer to chapter 23.4.

12.4 URL Groups

URL Groups enable the administrator to define HTTP rules easily (see chapter 10.2). For example, to disable access to a group of Web pages, you can simply define a URL group and assign permissions to the URL group, rather than defining permissions to each individual URL rule. URL groups can be defined in the *Configuration / Definitions / URL Groups* section.

To define URL rules go to the *URL Rules* tab in *Configuration → Content Filtering → HTTP Policy*.

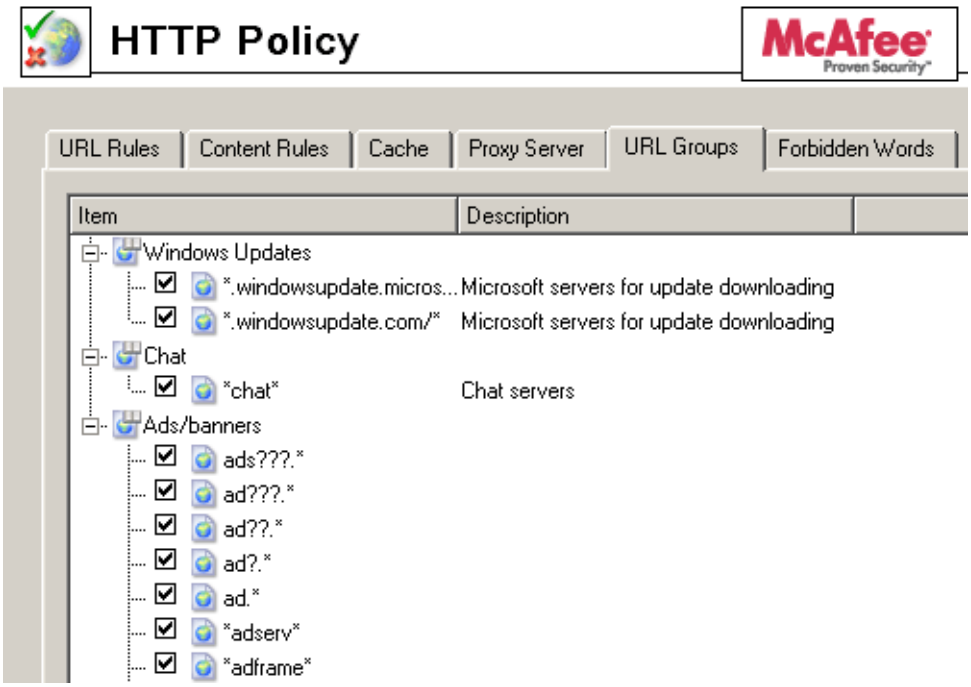


Figure 12.9 URL Groups

Matching fields next to names can be either checked to activate or unchecked to disable. This way you can deactivate URLs with no need to remove them and to define them again.

Note: The default *WinRoute* installation already includes a predefined URL group:

- *Ads/Banners* common URLs of pages that contain advertisements, banners, etc.

These groups are available to *WinRoute* administrators.

Click on the *Add* button to display a dialog where a new group can be created or a new URL can be added to existing groups.

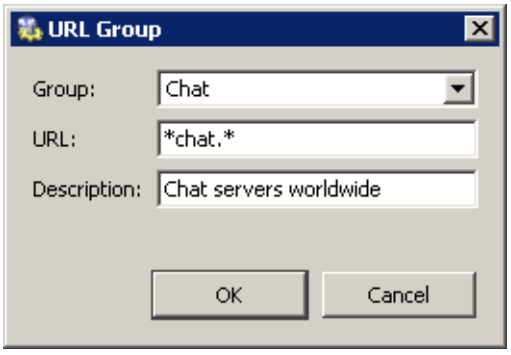


Figure 12.10 URL group definition

Group

Name of the group to which the URL will be added. This option enables the administrator to:

- select a group to which the URL will be added
- add a name to create a new group to which the URL will be included.

URL

The URL that will be added to the group. It can be specified as follows:

- full address of a server, a document or a web page without protocol specification (`http://`)
- use substrings with the special `*` and `?` characters. An asterisk stands for any number of characters, a question-mark represents one character.

Examples:

- `www.kerio.com/index.html` — a particular page
- `www.*` — all URL addresses starting with `www.` `www.*`
- `www.kerio.com` — all URLs at the `www.kerio.com` server (this string is equal to the `www.kerio.com/*` string)
- `*sex*` — all URL addresses containing the `sex` string
- `*sex??.cz*` — all URL addresses containing such strings as `sexxx.cz`, `sex99.cz`, etc.

Description

The URL description (comments and notes for the administrator).

Chapter 13

User Accounts and Groups

User accounts in *WinRoute* improve control of user access to the Internet from the local network. User accounts can be also used to access the *WinRoute* administration using the *Administration Console*.

WinRoute supports several methods of user accounts and groups saving, combining them with various types of authentication, as follows:

Internal user database

User accounts and groups and their passwords are saved in *WinRoute*. During authentication, usernames are compared to the data in the internal database.

This method of saving accounts and user authentication is particularly adequate for networks without a proper domain, as well as for special administrator accounts (user can authenticate locally even if the network communication fails).

On the other hand, in case of networks with proper domains (*Windows NT* or *Active Directory*), local accounts in *WinRoute* may cause increased demands on administration since accounts and passwords must be maintained twice (at the domain and in *WinRoute*).

Internal user database with authentication within the domain

User accounts are stored in *WinRoute*. However, users are authenticated at *Windows NT* or *Active Directory* domain (i.e. password is not stored in the user account in *WinRoute*). Obviously, usernames in *WinRoute* must match with the usernames in the domain.

This method is not so demanding as far as the administration is concerned. When, for example, a user wants to change the password, it can be simply done at the domain and the change will be automatically applied to the account in *WinRoute*. In addition to this, it is not necessary to create user accounts in *WinRoute* by hand, as they can be imported from a corresponding domain.

Import of user accounts from Active Directory

If Active Directory (Windows 2000 Server / Windows Server 2003) is used, automatic import of user accounts from it can be enabled. It is not necessary to define accounts in *WinRoute*, nor import them, since it is possible to configure templates by which specific parameters (such as access rights, content rules, transfer quotas, etc.) will be set for new *WinRoute* users. A corresponding user account will be automatically imported upon the first login of the user to *WinRoute*. Parameters set by using a template can be modified for individual accounts if necessary.

Note: This type of cooperation with *Active Directory* applies especially to older versions of *WinRoute* and makes these versions still compatible. In case of the first installation of *WinRoute*, it is recommended to apply transparent cooperation with *Active Directory*.

Transparent cooperation with Active Directory (Active Directory mapping)

WinRoute can use accounts and groups stored in *Active Directory* directly — no import to the local database is performed. Specific *WinRoute* parameters are added by the template of the corresponding account. These parameters can also be edited individually.

This type is the least demanding from the administrator's point of view (all user accounts and groups are managed in *Active Directory*) and it is the only one that allows using accounts from multiple *Active Directory* domains.

Note: In cases when users are authenticated at the domain (all described types excluding the first one), it is recommended to create at least one local account in *WinRoute* that has both read and write rights, or keep the original `Admin` account. This account provides connection to the *WinRoute* administration in case of the network or domain server failure.

13.1 Viewing and definitions of user accounts

To define local user accounts, import accounts to the local database or/and configure accounts mapped from the domain, go to the *User Accounts* tab in the *Users and Groups* → *Users* section.

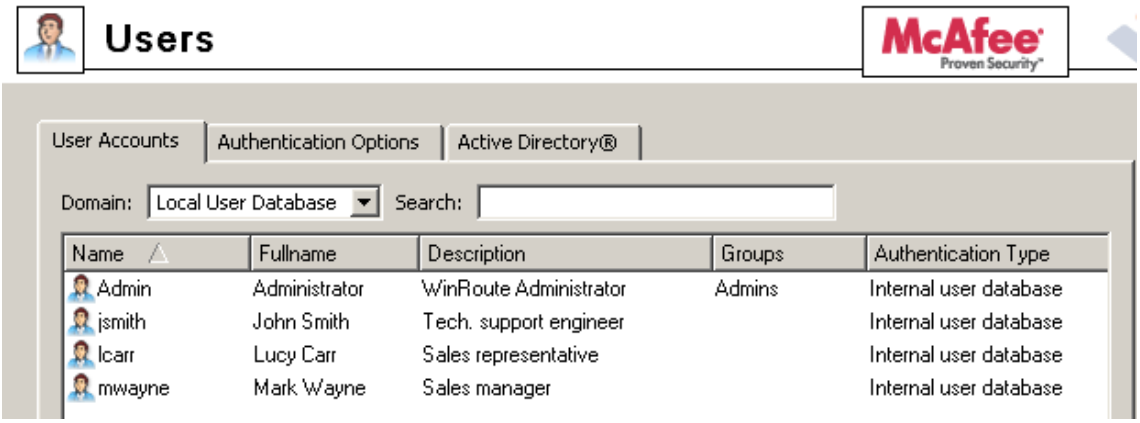


Figure 13.1 WinRoute user accounts

Domain

Use the *Domain* option to select a domain for which user accounts as well as other parameters will be defined. This item provides a list of mapped *Active Directory* domains (see chapter 13.4) and the local (internal) user database.

Search

The *Search* engine can be used to filter out user accounts meeting specified criteria. The searching is interactive — each symbol typed or deleted defines the string which is evaluated immediately and all accounts including the string in either *Name*, *Full name* or *Description* are viewed. The icon next to the entry can be clicked to clear the filtering string and display all user accounts in the selected domain (if the *Search* entry is blank, the icon is hidden).

The searching is helpful especially when the domain includes too many accounts which might make it difficult to look up particular items.

Hiding / showing disabled accounts

It is possible to disable accounts in *WinRoute*. Check the *Hide disabled user accounts* to show only active (enabled) accounts.

Account template

Parameters shared by the most accounts can be defined by a template. Templates simplify administration of user accounts — shared parameters are set just once, when defining the template. It is also possible to configure some accounts (such as administrator accounts) separately, without using the template.

Templates apply to specific domains (or to the local user database). Each template includes parameters of user rights, data transfer quota and rules for content rules (for detailed description of all these parameters, refer to chapter 13.2).

Local user accounts

If the *Local user database* is selected in the *Domain* item, user accounts in *WinRoute* are listed (complete information on these accounts are stored in the *WinRoute* configuration database). The following options are available for accounts in the local database:

Add, Edit, Remove

Click *Add*, *Edit* or *Remove* to create, modify or delete local user accounts (for details, see chapter 13.2). It is also possible to select more than one account by using the `Ctrl` and `Shift` keys to perform mass changes of parameters for all selected accounts.

Importing accounts from a domain

Accounts can be imported to the local database from the *Windows NT* domain or from *Active Directory*. Actually, this process includes automatic copying of domain accounts (account authenticating at the particular domain) to newly created

local accounts. For detailed information about import of user accounts, refer to chapter 13.3.

Import of accounts is recommended in case of the *Windows NT* domain. If *Active Directory* domain is used, it is recommended to use the transparent cooperation with *Active Directory* (domain mapping — see chapter 13.4).

Accounts mapped from the Active Directory domain

If any of the *Active Directory* domain is selected as *Domain*, user accounts in this domain are listed.

Edit User

For mapped accounts, specific *WinRoute* parameters can be set (refer to chapter 13.2). These settings are stored in the *WinRoute's* configuration database. Information stored in *Active Directory* (username, full name, email address) and authentication method cannot be edited.

Note: It is also possible to select more than one account by using the `Ctrl` and `Shift` keys to perform mass changes of parameters for all selected accounts.

In mapped *Active Directory* domains, it is not allowed to create or/and remove user accounts. These actions must be performed in the *Active Directory* database on the relevant domain server. It is also not possible to import user accounts — such an action would take no effect in case of a mapped domain.

13.2 Local user accounts

Local accounts are accounts created in the *Administration Console* or imported from a domain. These accounts are stored in the *WinRoute's* configuration database (in the `users.cfg` file under the *WinRoute's* installation directory). These accounts can be useful especially in domainless environments or for special purposes (e.g. firewall's administration).

Regardless on the method used for creation of the account, each user can be authenticated through the *WinRoute's* internal database, Active Directory or NT domain.

A basic administrator account is created during the *WinRoute* installation process. This account has full rights for *WinRoute* administration. It can be removed if there is at least one other account with full administration rights.

Warning:

1. All passwords should be kept safe and secret, otherwise they might be misused by an unauthorized person.

2. If all accounts with full administration rights are removed and connection to *Administration Console* is closed, it is not possible to connect to the *WinRoute* administra-

tion any longer. Under these conditions, a local user account (`Admin` with a blank password) will be created automatically upon the next start of the *WinRoute Firewall Engine*.

3. If the administration password is forgotten, contact our technical support at `http://www.kerio.com/`.

Creating a local user account

Open the *User Accounts* tab in the *User and groups* → *Users* section. In the *Domain* combo box, select *Local User Database*.

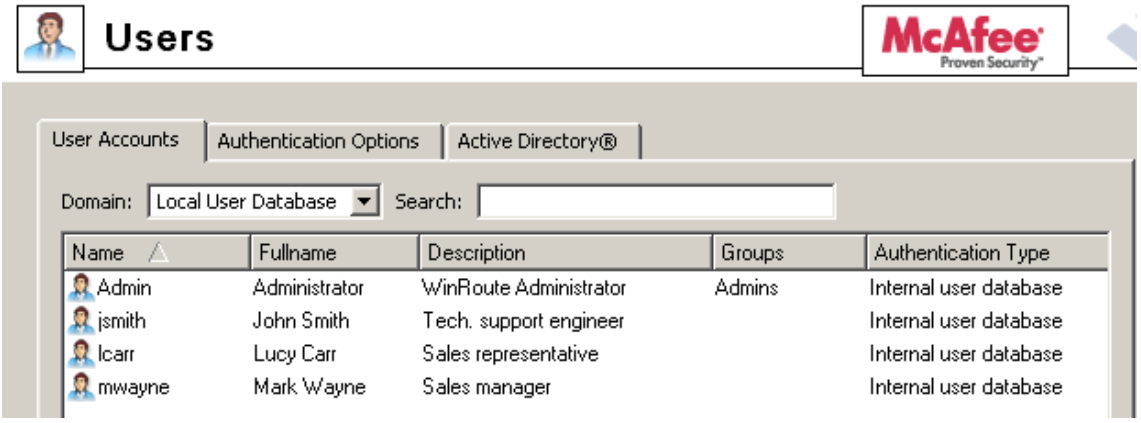


Figure 13.2 Local user accounts in WinRoute

Click on the *Add* button to open a guide to create a new user account.

Step 1 — basic information

Name

Username used for login to the account.
Warning: Usernames are not case-sensitive. We recommend not to use special characters (non-English languages) which might cause problems when authenticating at the Web interface.

Full Name

A full name of the user (usually first name and surname).

Description

User description (e.g. a position in a company).
The *Full Name* and the *Description* items have informative values only. Any type of information can be included or the field can be left empty.

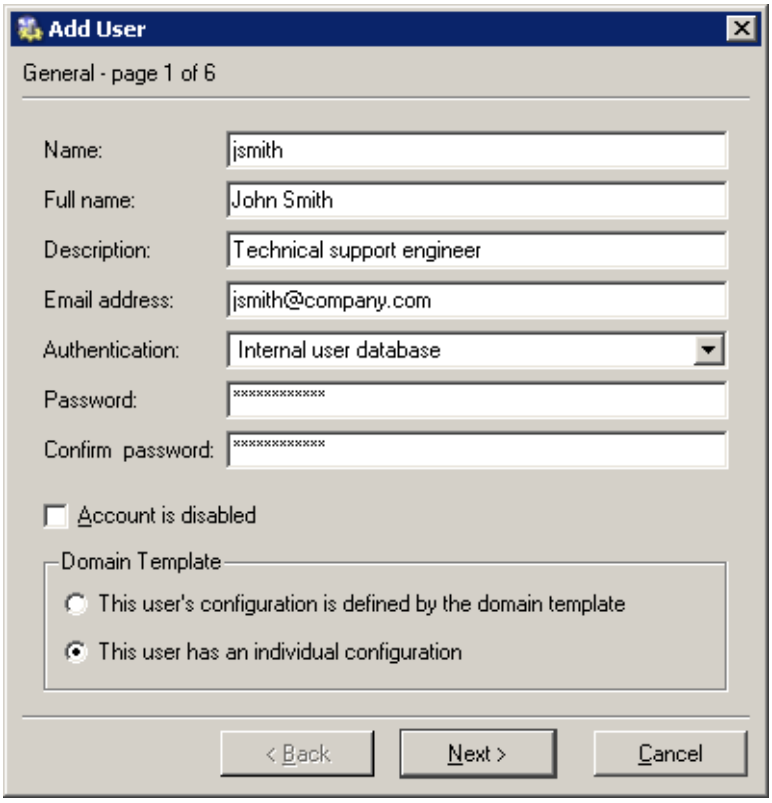


Figure 13.3 Creating a user account — basic parameters

Email Address

Email address of the user that alerts (see chapter 17.3) and other information (e.g.alert if a limit for data transmission is exceeded, etc.) will be sent to. A valid email address should be set for each user, otherwise some of the *WinRoute* features may not be used efficiently.

Note: A relay server must be set in *WinRoute* for each user, otherwise sending of alert messages to users will not function. For details, refer to chapter 16.4.

Authentication

User authentication (see below)

Account is disabled

Temporary blocking of the account so that you do not have to remove it.

Note: For example, this option can be used to create a user account for a user that will not be used immediately (e.g. an account for a new employee who has not taken up yet).

Domain template

Define parameters for the corresponding user account (access rights, data transfer quotas and content rules). These parameters can be defined by the template of

the domain (see chapter 13.1) or they can be set especially for the corresponding account.
Using a template is suitable for common accounts in the domain (common user accounts). Definition of accounts is simpler and faster, if a template is used.
Individual configuration is recommended especially for accounts with special rights (e.g. *WinRoute* administration accounts). Usually, there are not many such accounts which means their configuration comfortable.

Authentication options:

Internal user database

User account information is stored locally to *WinRoute*. In such a case, specify the *Password* and *Confirm password* items (later, the password can be edited in the Web interface — see chapter 9).
Warning:

1. Passwords may contain printable symbols only (letters, numbers, punctuation marks). Password is case-sensitive. We recommend not to use special characters (non-English languages) which might cause problems when authenticating via the Web interface.
2. NTLM authentication cannot be used for automatic authentication method by NTLM (refer to chapter 23.3).. These accounts also cannot be used for authentication to the *Clientless SSL-VPN* interface (see chapter 22).

NT domain / Kerberos 5

Users are authenticated through the Windows NT domain (Windows NT 4.0) or through the Active Directory (Windows 2000/2003).
Go to the *Users* section of the *Active Directory / NT domain* tab to set parameters for user authentication through the NT domain or through the Active Directory. If Active Directory authentication is set also for NT domain, it will be preferred.
Note: User accounts with this type of authentication set will not be active unless authentication through Active Directory or/and NT domain is enabled. For details, see chapter 13.3.

Step 2 — groups

Groups into which the user will be included can be added or removed with the *Add* or the *Remove* button within this dialog (to create new groups go to *User and Groups* → *Groups* — see chapter 13.5). Follow the same guidelines to add users to groups during group definition. It is not important whether groups or users are defined first.

HINT: While adding new groups you can mark more than one group by holding either the *Ctrl* or the*Shift* key.

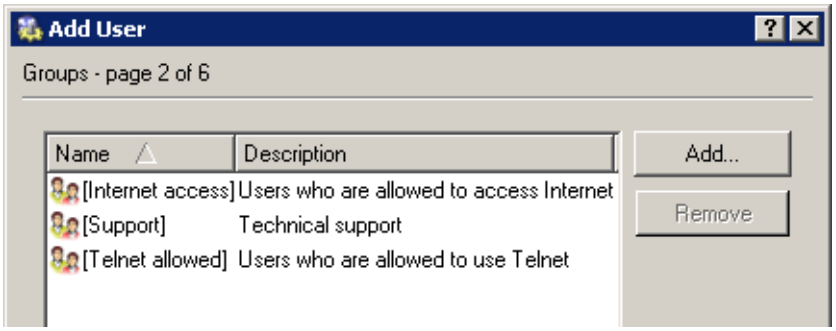


Figure 13.4 Creating a new user account — groups

Step 3 — access rights

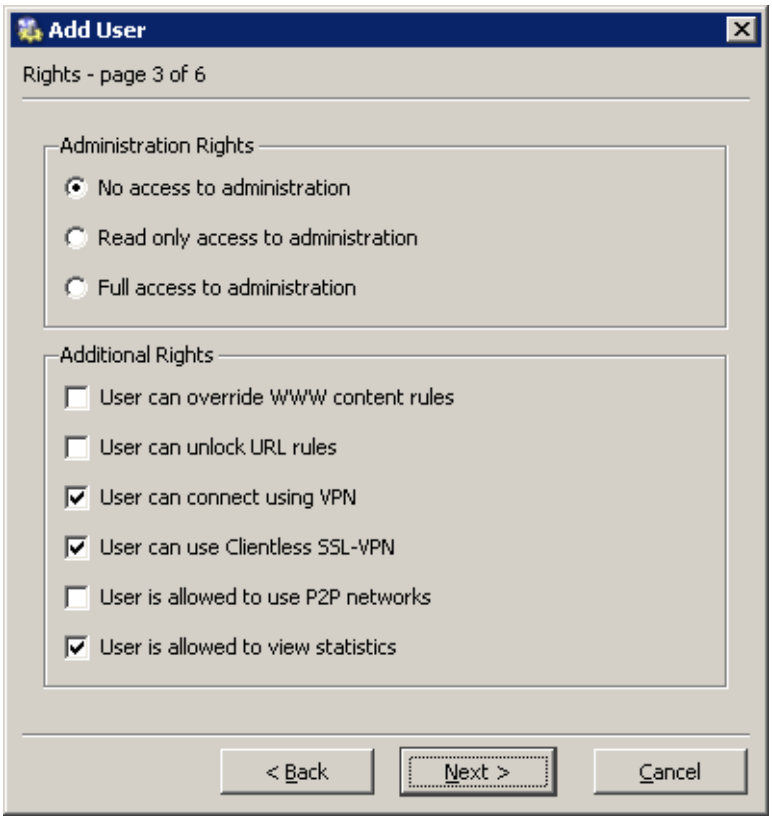

Add User
Rights - page 3 of 6
Administration Rights
No access to administration
Read only access to administration
Full access to administration
Additional Rights
User can override WWW content rules
User can unlock URL rules
User can connect using VPN
User can use Clientless SSL-VPN
User is allowed to use P2P networks
User is allowed to view statistics
< Back
Next >
Cancel

Figure 13.5 Creating a new user account — user rights

Each user must be assigned one of the following three levels of access rights.

No access to administration
The user has no rights to access the *WinRoute* administration. This setting is commonly used for the majority of users.

Read only access to administration
The user can access *WinRoute*. He or she can read settings and logs but cannot edit them.

Full access to administration
The user can read or edit all the records and settings and his or her rights are equal to the administrator rights (`Admin`). If there is at least one user with the full access to the administration, the default `Admin` account can be removed.

Additional rights:

User can override WWW content rules
User can customize personal Web content filtering settings independently of the global configuration (for details, refer to *Step 4* and to chapter 9.4).

User can unlock URL rules
If this option is checked, the user is allowed to bypass the rule denying access to the queried website — at the page providing information about the denial, the *Unlock* button is displayed. The unlock feature must also be enabled in the corresponding URL rule (for details, refer to chapter 10.2).

User can connect using VPN
The user is allowed to connect through *WinRoute's* VPN server (using *Kerio VPN Client*). For detailed information, see chapter 21.

User can use Clientless SSL-VPN
The user will be allowed to access shared files and folders in the local network via the *Clientless SSL-VPN* web interface. For details, see chapter 22.

User is allowed to use P2P networks
Traffic of this user will not be blocked if *P2P* (*Peer-to-Peer*) networks are detected. For details, see chapter 15.1.

User is allowed to view statistics
This user will be allowed to view firewall statistics in the web interface (see chapter 9).

HINT: Access rights can also be defined by a user account template.

Step 4 — data transmission quota

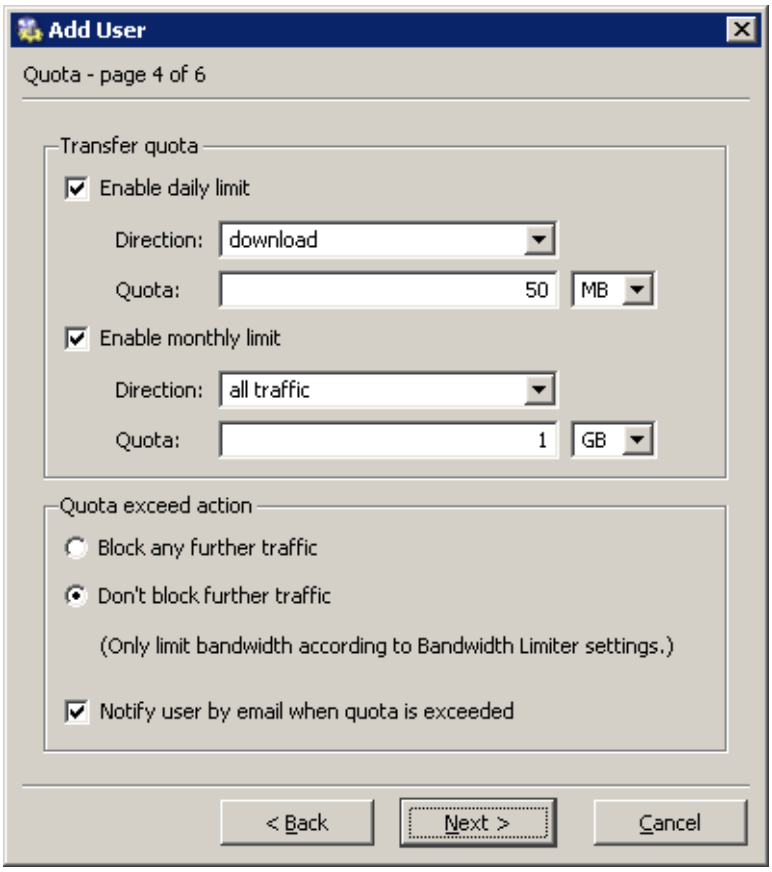


Figure 13.6 Creating a new user account — data transmission quota

Daily and monthly limit for volume of data transferred by a user, as well as actions to be taken when the quota is exceeded, can be set in this section.

Transfer quota

Limit settings

- *Enable daily limit* — daily limit parameters.
  Use the *Direction* combo box to select which transfer direction will be controlled (*download* — incoming data, *upload* — outgoing data, *all traffic* — both incoming and outgoing data).
  The limit can be set in the *Quota* entry using megabytes or gigabytes.
- *Enable monthly limit* — monthly limit parameters. To set this quota, follow the same instructions as for the daily limit.

Quota exceed action

Set actions which will be taken whenever a quota is exceeded:

- *Block any further traffic* — the user will be allowed to continue using the opened connections, however, will not be allowed to establish new connections (i.e. to connect to another server, download a file through FTP, etc.)
- *Don't block further traffic (Only limit bandwidth...)* — Internet connection speed (so called bandwidth) will be limited for the user. Traffic will not be blocked but the user will notice that the Internet connection is slower than usual (this should make such users to reduce their network activities). For detailed information, see chapter 7.

Check the *Notify user by email when quota is exceeded* option to enable sending of warning messages to the user in case that a quota is exceeded. A valid email address must be specified for the user (see *Step 1*). SMTP Relay must be set in *WinRoute* (see chapter 16.4).

If you wish that your *WinRoute* administrator is also notified when a quota is almost exceeded, set the alert parameters in *Configuration* → *Accounting*. For details, refer to chapter 17.3.

Notes:

1. If a quota is exceeded and the traffic is blocked in result, the restrictions will continue being applied until the end of the quota period (day or month). To cancel these restrictions before the end of a corresponding period, the following actions can be taken:
   - disable temporarily a corresponding limit, raise its value or switch to the *Don't block further traffic* mode
   - reset statistics of a corresponding user (see chapter 18.2).
2. Actions for quota-exceeding are not applied if the user is authenticated at the firewall. This would block all firewall traffic as well as all local users. However, transferred data is included in the quota!

HINT: Data transfer quota and actions applied in response can also be set by a user account template.

Step 5 — content rules

Within this step special content filter rules settings for individual users can be defined. Global rules (defined in the *Content Rules* tab in the *Configuration* → *Content Filtering* → *HTTP Policy* section) are used as default (when a new user account is defined). For details, see chapter 10.3.

Note: These settings can be customized at a corresponding page of the *WinRoute's* Web interface (see chapter 9.4). If the user can override content rules, any changes can be

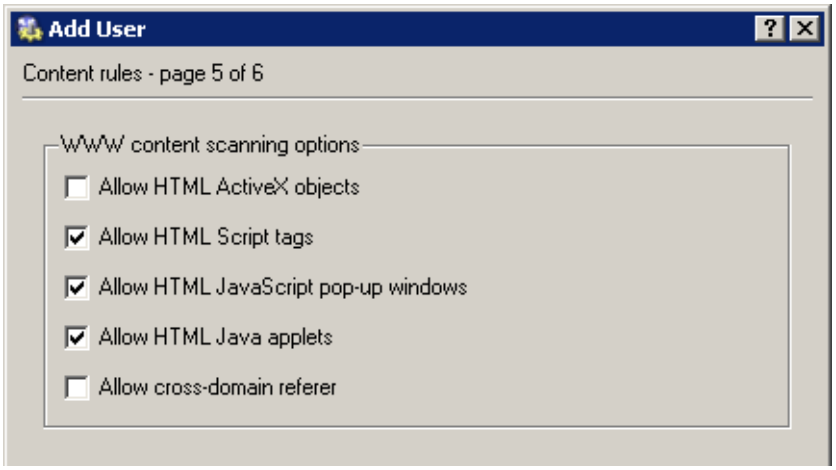

Add User
Content rules - page 5 of 6
WWW content scanning options
Allow HTML ActiveX objects
Allow HTML Script tags
Allow HTML JavaScript pop-up windows
Allow HTML Java applets
Allow cross-domain referer

Figure 13.7 Creating a new user account — Web site content rules

made. Users who are not allowed to override rules can enable or/and disable only features which are available for them (set in their personal configuration).

HINT: Content rules can also be defined by a user account template.

Step 6 — user's IP addresses

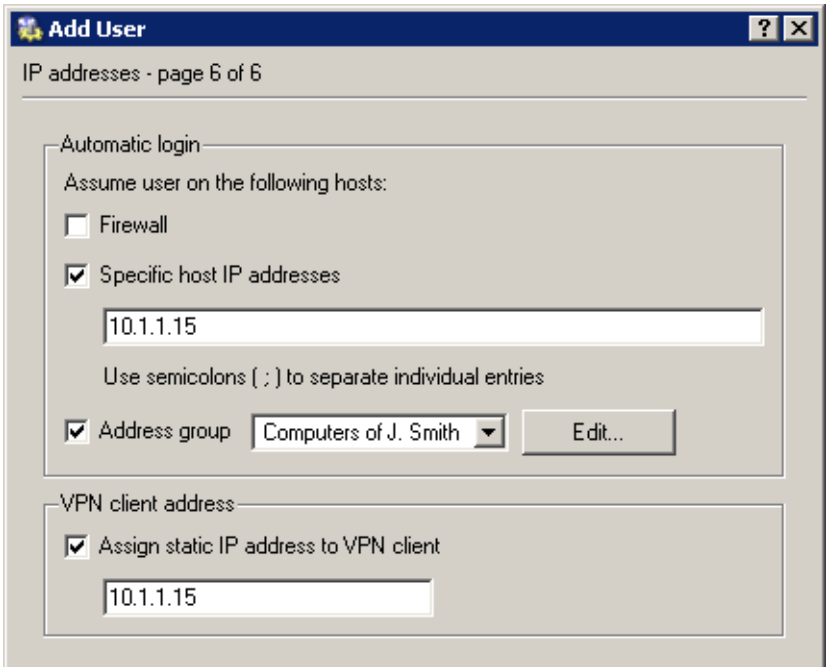


Figure 13.8 Creating a new user account — IP addresses for VPN client and automatic logins

If a user works at a reserved workstation (i.e. this computer is not by any other user) with a fixed IP address (static or reserved at the DHCP server), the user can use automatic login from the particular IP address. This implies that whenever a connection attempt from this IP address is detected, *WinRoute* assumes that the connection is performed by the particular user and it does not require authentication. The user is logged-in automatically and all functions are available as if connected against the username and password.

This implies that only one user can be automatically authenticated from a particular IP address. When a user account is being created, *WinRoute* automatically detects whether the specified IP address is used for automatic login or not.

Automatic login can be set for the firewall (i.e. for the *WinRoute* host) or/and for any other host(s) (i.e. when the user connects also from an additional workstation, such as notebooks, etc.). An IP address group can be used for specification of multiple hosts (refer to chapter 12.1).

Warning: Automatic login decreases user's security. If an unauthorized user works on the computer for which automatic login is enabled, he/she uses the identity of the host's user who is authenticated automatically. Therefore, automatic login should be accompanied by another security feature, such as by user login to the operating system.

IP address which will be always assigned to the VPN client of the particular user can be specified under *VPN client address*. Using this method, a fixed IP address can be assigned to a user when he/she connects to the local network via the *Kerio VPN Client*. It is possible to add this IP to the list of IP addresses from which the user will be authenticated automatically.

For detailed information on the *Kerio Technologies'* proprietary VPN solution, refer to chapter 21.

Editing User Account

The *Edit* button opens a dialog window where you can edit the parameters of the user account. This dialog window contains all of the components of the account creation guide described above, divided into tabs in one window.

13.3 Local user database: external authentication and import of accounts

User in the local database can be authenticated either at the *Active Directory* domain or at the *Windows NT* domain (see chapter 13.2, step one). To enable these authentication methods, corresponding domains must be set in the *Local User Database* section on the *Authentication Options* tab.

Figure 13.9 Setting domains for authentication of local accounts

Active Directory

Use the *Enable Active Directory authentication* option to enable/disable user authentication at the local database in the selected *Active Directory* domain.

The following conditions must be met to enable smooth functionality of user authentication through Active Directory:

1. The *WinRoute* host must be a member of this domain.

2. The Active Directory domain controller (server) must be set as the primary DNS server.

   If the DNS server itself is set in the operating system, the domain controller of the Active Directory must be the first item in the DNS servers list in the *DNS Forwarder* configuration (for details, refer to chapter 5.3).

Note: Users can also be authenticated in any domain set as trustworthy for the particular domain.

NT domain

Use the *Enable NT domain authentication* option to enable *NTLM* authentication for the domain selected.

Warning:

1. The host where *WinRoute* is installed must belong to this domain.

2. Authentication through a corresponding NT domain must be allowed to enable NTLM authentication through Web browsers (refer to chapter 8.1). For the Windows 2000/2003 domain, it is necessary to set authentication both through *Active Directory* and NT domain.

Automatic import of user accounts from Active Directory

If *Active Directory* is used, automatic import of user accounts can be applied. Specific *WinRoute* parameters (such as access rights, content rules, data transfer quotas, etc.) can be set by using the template for the local user database (see chapter 13.1) or/and they can be defined individually for special accounts. A corresponding user account will be imported upon the first login of the user to *WinRoute*.

Note: This type of user accounts import should, above all, help to keep compatibility with older versions of *WinRoute*. It is much easier and more recommended to use transparent support for *Active Directory* (domain mapping — refer to chapter 13.4).

User accounts will be imported from the domain specified in the *Active Directory domain name* entry. Click *Configure automatic import* to set parameters for this function.

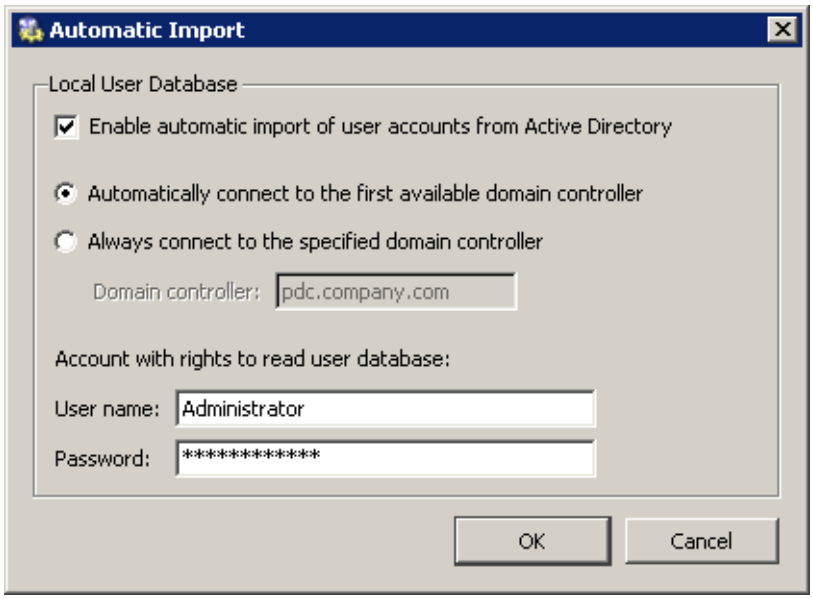


Figure 13.10 Configuration of automatic import of user accounts from Active Directory

For imports of accounts, it is necessary that *WinRoute* knows the domain server of the corresponding *Active Directory* domain. *WinRoute* can either detect it automatically or it can always connect to a specified server. The automatic connection to the first server available increases reliability of the connection and eliminates problems in cases when a domain controller fails. The other option (specification of a controller) is recommended for domains with one server only (speeds the process up).

It is also necessary to enter login data of a user with read rights for the *Active Directory* database (any user account belonging to the corresponding domain).

Note: It is not possible to combine the automatic import with *Active Directory* domain mapping (see chapter 13.4) as the local user database would collide with the mapped domain. If possible, it is recommended to use the *Active Directory* mapping alternative.

Manual import of user accounts

It is also possible to import special accounts to the local database from the *Windows NT* domain or from *Active Directory*. Each import of a user account covers creating of a local account with the identical name and the same domain authentication parameters. Specific *WinRoute* parameters (such as access rights, content rules, data transfer quotas, etc.) can be set by using the template for the local user database (see chapter 13.1) or/and they can be defined individually for special accounts. The *Windows NT / Active Directory* authentication type is set for all accounts imported..

Note: This method of user accounts import is recommended especially when *Windows NT* domain is used (domain server with the *Windows NT Server* operating system). If *Active Directory* domain is used, it is easier and recommended to use the transparent support for *Active Directory* (domain mapping — see chapter13.4).

Click *Import* on the *User Accounts* tab to start importing user accounts. In the import dialog, select the type of the domain from which accounts will be imported and, with respect to the domain type, specify the following parameters:

- *NT domain* — domain name is required for import. The *WinRoute* host must be a member of this domain.

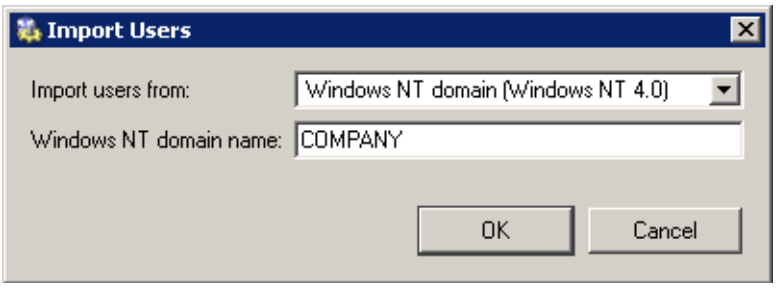


Figure 13.11 Importing accounts from the Windows NT domain

- *Active Directory* — for import of accounts, *Active Directory* domain name, DNS name or IP address of the domain server as well as login data for user database reading (any account belonging to the domain) are required.

When connection with the corresponding domain server is established successfully, all accounts in the selected domain are listed. When accounts are selected and the selection is confirmed, the accounts are imported to the local user database.

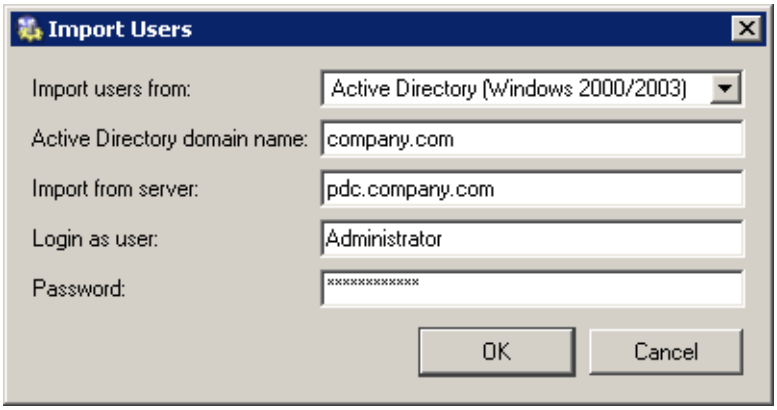


Figure 13.12 Import of accounts from Active Directory

13.4 Active Directory domains mapping

In *WinRoute*, it is possible to directly use user accounts from one or more *Active Directory* domain(s). This feature is called either transparent support for *Active Directory* or *Active Directory* domain(s) mapping. The main benefit of this feature is that the entire administration of all user accounts and groups is maintained in *Active Directory* only (using standard system tools). In *WinRoute*, a template can be defined for each domain that will be used to set specific *WinRoute* parameters for user accounts (access rights, data transfer quotas, content rules — see chapter 13.1). If needed, these parameters can also be set individually for any accounts.

Note: The *Windows NT* domain cannot be mapped as described. In case of the *Windows NT* domain, it is recommended to import user accounts to the local user database (refer to 13.3)

Domain mapping requirements

The following conditions must be met to enable smooth functionality of user authentication through Active Directory domains:

- For mapping of one domain:

  1. The *WinRoute* host must be a member of the corresponding *Active Directory* domain.

  2. The Active Directory domain controller (server) must be set as the primary DNS server.

If the DNS server itself is set in the operating system, the domain controller of the *Active Directory* must be the first item in the DNS servers list in the *DNS Forwarder* configuration (for details, refer to chapter 5.3).

- For mapping of multiple domains:

  1. The *WinRoute* host must be a member of one of the mapped domains.

  2. It is necessary that this domain trusts any other domains mapped in *WinRoute* (for details, see the documentation regarding the operating system on the corresponding domain server).

  3. For DNS configuration, the same rules are followed as for mapping of a single domain (DNS server must be a domain server of the domain which the *WinRoute's* host belongs to).

Single domain mapping

To set *Active Directory* domain mapping, go to the *Active Directory* tab under *User and Groups* → *Users*.

If no domain mapping has been defined yet or only one domain is defined, the *Active Directory* tab already includes predefined parameters customized for the domain mapping.

Active Directory mapping

In the top part of the *Active Directory* tab, it is possible to enable/disable mapping of user accounts from the *Active Directory* domain to *WinRoute*.
The *Active Directory domain name* entry requires full DNS name of the mapped domain (e.g. `company.com`, `company` would not be satisfactory). For your better reference, it is also recommended to provide a short description of the domain (especially if more domains are mapped).

Domain Access

In the *Domain Access* section, specify the login user name and password of an account with read rights for the *Active Directory* database (any user account within the domain can be used, unless blocked).
Click *Advanced* to set parameters for communication with domain servers:

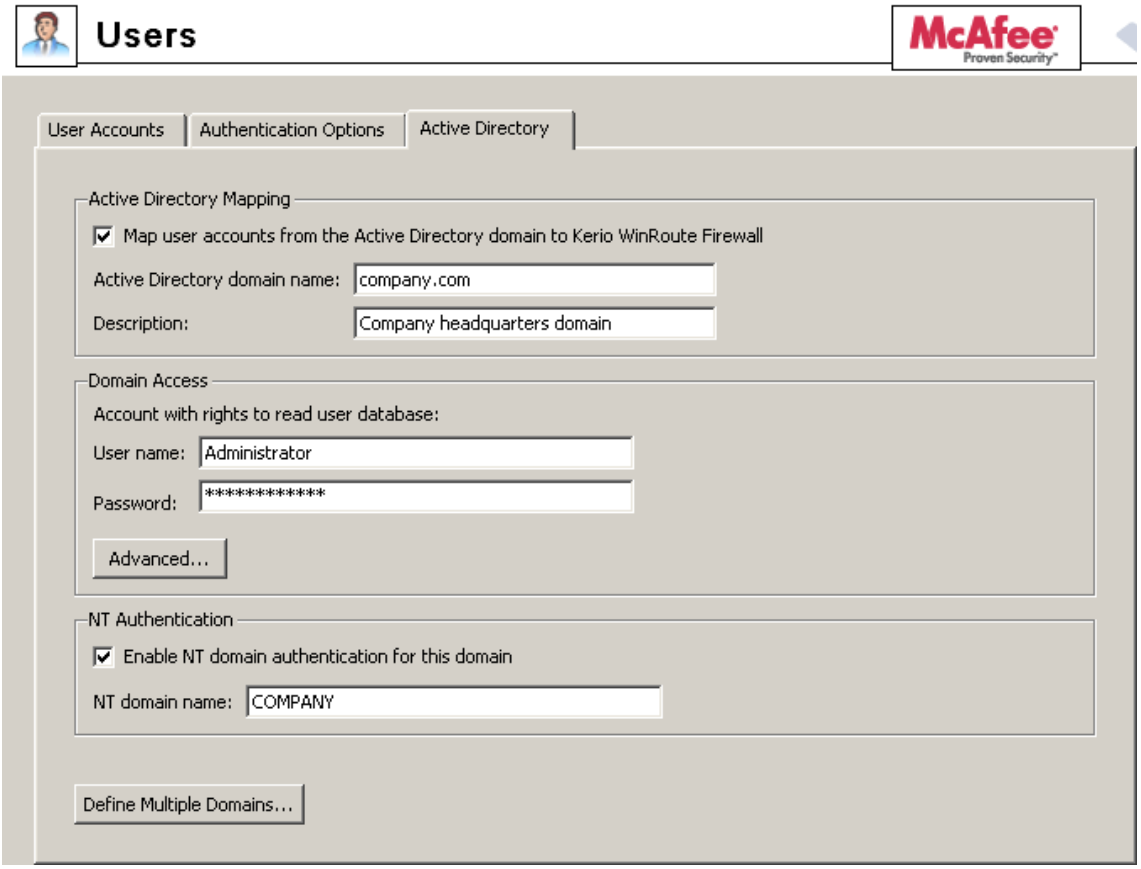


Figure 13.13 Active Directory domain mapping

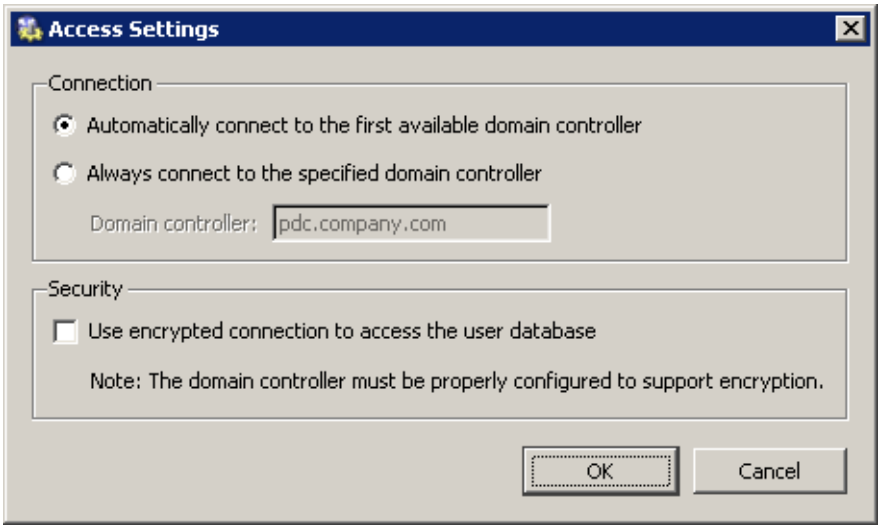


Figure 13.14 Advanced settings for access to the Active Directory

- It is possible to let *WinRoute* connect automatically to a specified server or to search for a domain server. The automatic connection to the first server avail-

able increases reliability of the connection and eliminates problems in cases when a domain controller fails. The other option (specification of a controller) is recommended for domains with one server only (speeds the process up).

- Encrypted connection — to increase security of the communication with the domain server, encrypted connection can be used (thus, the traffic cannot be tapped). In such a case, encrypted connection must be enabled at the domain server. For details, refer to documents regarding the corresponding operating system.

NT authentication support

For the *Active Directory* domain, *NTLM* is also available as an authentication method. This option is required if you intend to use automatic authentication in web browsers (see chapter 23.3).

For *NTLM* authentication, name of the NT domain corresponding with the domain specified in the *Active Directory* domain is required.

For mapping from multiple *Active Directory* domains, click on *Define Multiple Domains*.

Multiple domains mapping

Click *Define Multiple Domains* to switch the *Active Directory* tab to the mode where domains are listed.

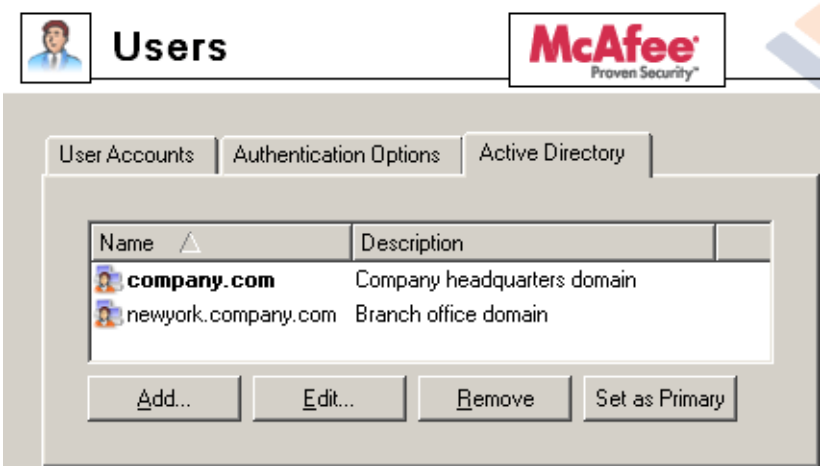


Figure 13.15 Mapping of multiple Active Directory domains

One domain is always set as primary. In this domain, all user accounts where the domain is not specified, will be searched (e.g. `jsmith`). Users of other domains must login by username including the domain (e.g. `drdolittle@usoffice.company.com`).

Use the *Add* or the *Edit* button to define a new domain. This dialog includes the same parameters as the *Active Directory* tab in administration of an only domain (see above).

Notes:

1. By default, the domain defined first is set as primary. You can use the *Set as primary* button to set the selected domain as primary.

2. Membership of *WinRoute* in the domain is not necessarily required for primary domains (see *Domain mapping requirements*). Settings of the primary domain only define which users will be allowed to login to *WinRoute* (i.e. to the web interface, to the *SSL-VPN* interface, to the *WinRoute* administration, etc.) using the username without domain.

Collision of Active Directory with the local database and conversion of accounts

During *Active Directory* domain mapping, collision with the local user database may occur if a user account with an identical name exists both in the domain and in the local database. If multiple domains are mapped, a collision may occur only between the local database and the primary domain (accounts from other domains must include domain names which make the name unique).

If a collision occurs, a warning is displayed at the bottom of the *User Accounts* tab. Click on the link in the warning to convert selected user accounts (to replace local accounts by corresponding *Active Directory* accounts).

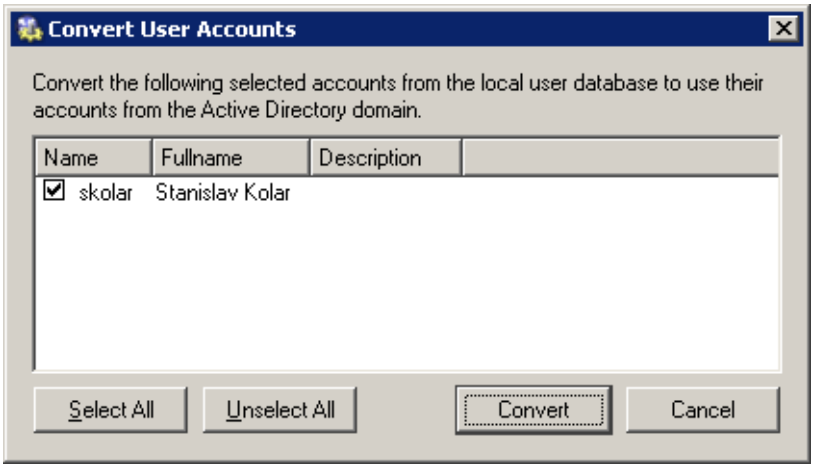


Figure 13.16 Conversion of user accounts

The following operations will be performed automatically within each conversion:

- substitution of any appearance of the local account in the *WinRoute* configuration (in traffic rules, URL rules, FTP rules, etc.) by a corresponding account from the *Active Directory* domain,
- removal of the account from the local user database.

Accounts not selected for the conversion are kept in the local database (the collision is still reported). Colliding accounts can be used — the accounts are considered as two independent accounts. However, under these circumstances, *Active Directory* accounts must be always specified including the domain (even though it belongs to the primary domain); username without the domain specified represents an account belonging to the local database. However, as long as possible, it is recommended to remove all collisions by the conversion.

Note: In case of user groups, collisions do not occur as local groups are always independent from the *Active Directory* (even if the name of the local group is identical with the name of the group in the particular domain).

13.5 User groups

User accounts can be sorted into groups. Creating user groups provides the following benefits:

- Specific access rights can be assigned to a group of users. These rights complement rights of individual users.
- Each group can be used when traffic and access rules are defined. This simplifies the definition process so that you will not need to define the same rule for each user.

User groups Definitions

User groups can be defined in *User and Groups* → *Groups*.

Domain

Use the *Domain* option to select a domain for which user accounts or other parameters will be defined. This item provides a list of mapped *Active Directory* domains (see chapter 13.4) and the local user database.
In *WinRoute*, it is possible to create groups only in the local user database. It is not possible to create groups in mapped *Active Directory* domains. It also not possible to import groups from the *Windows NT* domain or from *Active Directory*.
In case of groups mapped in *Active Directory* domains, it is possible to set only access rules (see below — step 3 of the user group definition wizard).

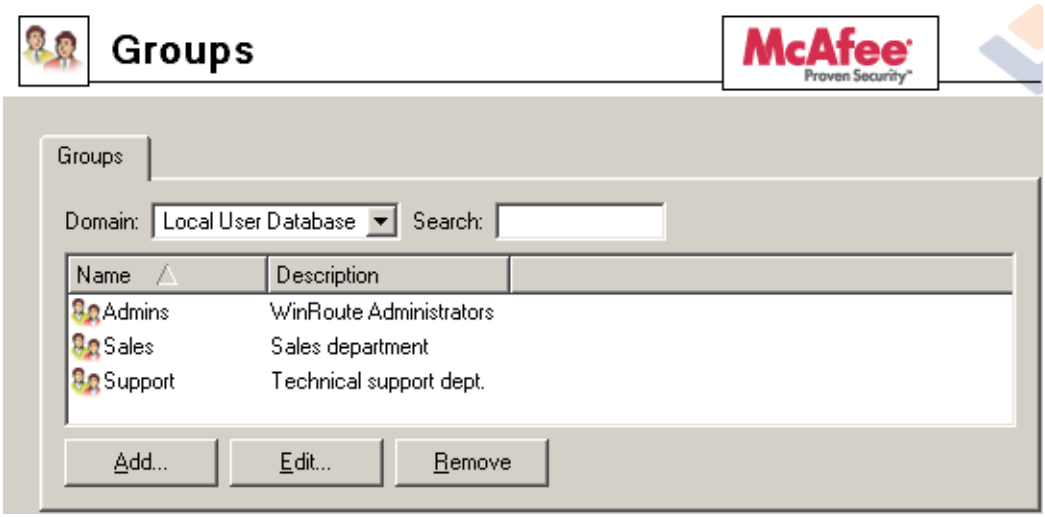


Figure 13.17 WinRoute user groups

Search

The *Search* engine can be used to filter out user groups meeting specified criteria. The searching is interactive — each symbol typed or deleted defines the string which is evaluated immediately and all groups including the string in either *Name* or *Description* are viewed. The icon next to the entry can be clicked to clear the filtering string and display all groups in the selected domain (if the *Search* entry is blank, the icon is hidden).

The searching is helpful especially when the domain includes too many groups which might make it difficult to look up particular items.

Creating a new local user group

In the *Domain* combo box in *Groups*, select Local User Database.

Click *Add* to start a wizard where a new user group can be created.

Step 1 — Name and description of the group

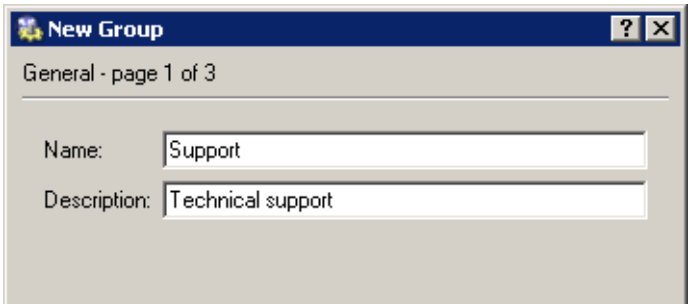


Figure 13.18 Creating a user group — basic parameters

Name
Group name (group identification).

Description
Group description. It has an informative purpose only and may contain any information or the field can be left empty.

Step 2 — group members

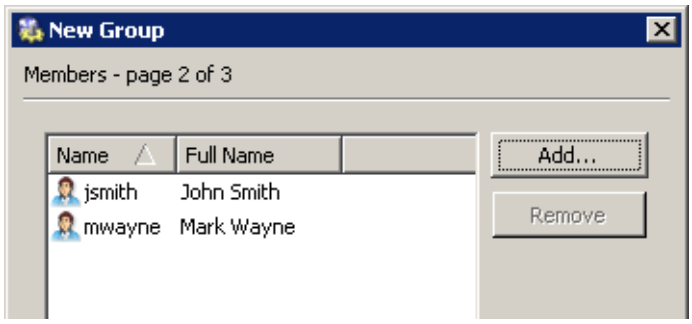


Figure 13.19 Creating a user group — adding user accounts to the group

Using the *Add* and *Remove* buttons you can add or remove users to/from the group. If user accounts have not been created yet, the group can be left empty and users can be added during the account definition (see chapter 13.1).

HINT: To select more than one user hold the *Ctrl* or the *Shift* key.

Step 3 — group access rights

The group must be assigned one of the following three levels of access rights:

No access to administration
Users included in this group cannot access the *WinRoute* administration.

Read only access
Users included in this group can access the *WinRoute* administration. However, they can only read the records and settings and they are not allowed to edit them.

Full access to administration
Users in this group have full access rights.

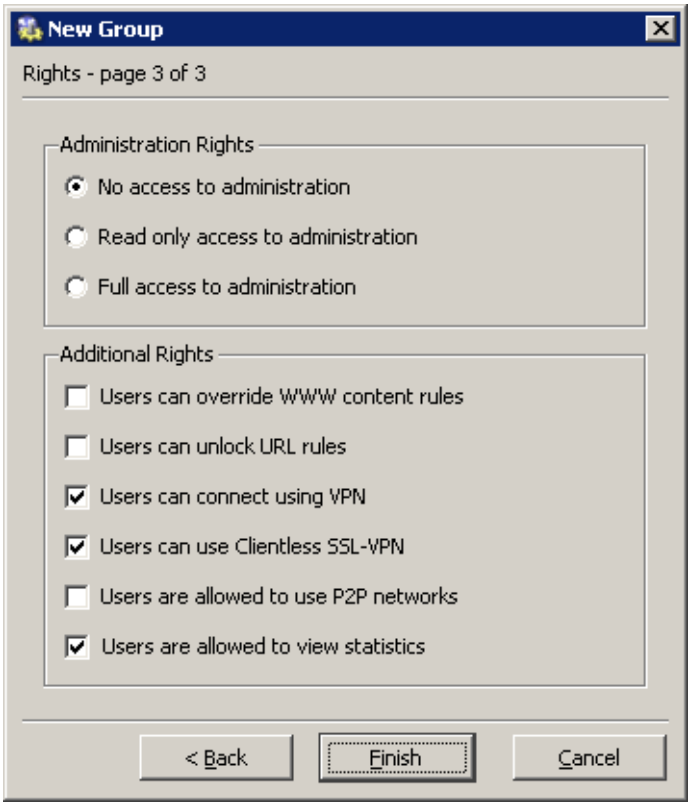


Figure 13.20 Creating a user group — members' user rights

Additional rights:

Users can override WWW content rules
: User belonging to the group can customize personal Web content filtering settings independently of the global configuration (for details see chapters 10.3 a 9.4).

User can unlock URL rules
: This option allows its members one-shot bypassing of denial rules for blocked websites (if allowed by the corresponding URL rule — see chapter 10.2). All performed unlock actions are traced in the *Security* log.

Users can connect using VPN
: Members of the group can connect to the local network via the Internet using the *Kerio VPN Client* (for details, see chapter 21).

User can use Clientless SSL-VPN
: Members of this group will be allowed to access shared files and folders in the local network via the *Clientless SSL-VPN* web interface. For details, see chapter 22.

Users are allowed to use P2P networks

The *P2P Eliminator* module (detection and blocking of *Peer-to-Peer* networks — see chapter 15.1) will not be applied to members of this group.

Users are allowed to view statistics

Users in this group will be allowed to view firewall statistics in the web interface (see chapter 9).

Group access rights are combined with user access rights. This means that current user rights are defined by actual rights of the user and by rights of all groups in which the user is included.

Chapter 14

Remote Administration and Update Checks

14.1 Setting Remote Administration

Remote administration can be either permitted or denied by definition of the appropriate traffic rule. Traffic between *WinRoute* and *Administration Console* is performed by TCP and UDP protocols over port 44333. The definition can be done with the predefined service *KWF Admin*.

If *WinRoute* includes only traffic rules generated by the wizard, remote administration is available through all interfaces except the one which is used for Internet connection and where NAT is enabled (see chapter 6.1). This means that remote administration is available from all local hosts.

How to allow remote administration from the Internet

In the following example we will demonstrate how to allow *WinRoute* remote administration from some Internet IP addresses.

- *Source* — group of IP addresses from which remote administration will be allowed.

  For security reasons it is not recommended to allow remote administration from an arbitrary host within the Internet (this means: do not set *Source* as the Web interface).

- *Destination* — *Firewall* (host where *WinRoute* is running)

- *Service* — *KWF Admin* (predefined service— *WinRoute* administration)

- *Action* — *Permit* (otherwise remote administration would be blocked)

- *Translation* — Because the engine is running on the firewall there is no need for translation.

Figure 14.1 Traffic rule that allows remote administration

HINT: The same method can be used to enable or disable remote administration of *Kerio MailServer* through *WinRoute* (the *KMS Admin* service can be used for this purpose).

Note: Be very careful while defining traffic rules, otherwise you could block remote administration from the host you are currently working on. If this happens, the connection between *Administration Console* and *WinRoute Firewall Engine* is interrupted (upon clicking on the *Apply* button in *Configuration* → *Traffic Policy*). Local connections (from the *WinRoute Firewall Engine's* host) works anyway. Such a traffic cannot be blocked by any rule.

14.2 Update Checking

WinRoute enables automatic check for new versions at the *Kerio Technologies* website. Whenever a new version is detected, is download and installation is offered.

Open the *Update Checker* tab in the *Configuration* → *Advanced Options* section to view information on a new version and to set parameters for automatic checks for new versions.

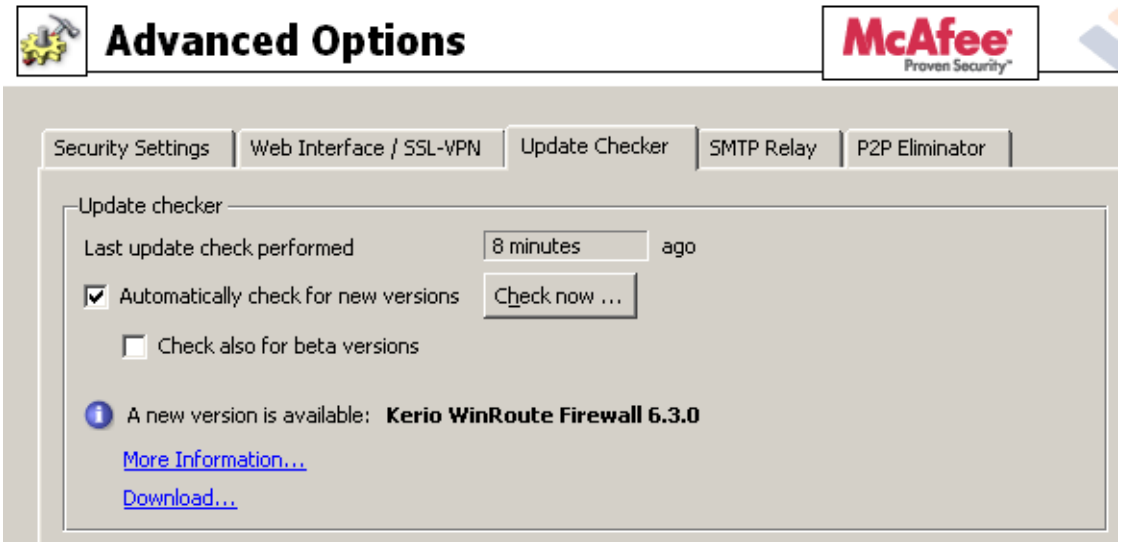


Figure 14.2 Check for new WinRoute versions

Last update check performed ... ago

Information on how much time ago the last update check was performed.

If the time is too long (several days) this may indicate that the automatic update checks fail for some reason (i.e. access to the update server is blocked by a traffic rule). In such cases we recommend you to perform a check by hand (by clicking on the *Check now* button), view results in the *Debug* log (see chapter 20.6) and take appropriate actions.

Check for new versions

Use this option to enable/disable automatic checks for new versions. Checks are performed:

- 2 minutes after each startup of the *WinRoute Firewall Engine*,
- and then every 24 hours.

Results of each attempted update check (successful or not) is logged into the *Debug* log (see chapter 20.6).

Check also for beta versions

Enable this option if you want *WinRoute* to perform also update checks for beta versions.

If you wish to participate in testing of *WinRoute* beta versions, enable this option. In case that you use *WinRoute* in operations in your company (i.e. at the Internet gateway of your company), we recommend you not to use this option (beta versions are not tested yet and they could endanger functionality of your networks, etc.).

Check now

Click on this button to check for updates immediately.

If a new version is available, detailed information links and download links (links to installation files) are provided:

- *More information* — this link opens *WinRoute* changelog page in the default web browser.
- *Download* — direct link to the particular version's installation file. Click the link to download the installation file in your default browser.

For detailed information on *WinRoute* installation, refer to chapter 2.3.

Note: Whenever a new version is detected, user is informed through the application and licence info dialog (the *Kerio WinRoute Firewall* item in the *Administration Console* tree). Clicking on link *New version available, click here for details...* switches the *Administration Console* to the *Update Checker* tab of the *Configuration* → *Advanced Options* section.

Figure 14.3 Administration Console's welcome page informing that a new version is available

Chapter 15

Advanced security features

15.1 P2P Eliminator

Peer-to-Peer (*P2P*) networks are world-wide distributed systems, where each node can represent both a client and a server. These networks are used for sharing of big volumes of data (this sharing is mostly illegal). *DirectConnect* and *Kazaa* are the most popular ones.

In addition to illegal data distribution, utilization of *P2P* networks overload lines via which users are connected to the Internet. Such users may limit connections of other users in the same network and may increase costs for the line (for example when volume of transmitted data is limited for the line).

WinRoute provides the *P2P Eliminator* module which detects connections to *P2P* networks and applies specific restrictions. Since there is a large variety of *P2P* networks and parameters at individual nodes (servers, number of connections, etc.) can be changed, it is hardly possible to detect all *P2P* connections.[5]. However, using various methods (such as known ports, established connections, etc.), the *P2P Eliminator* is able to detect whether a user connects to one or multiple *P2P* networks.

The following restrictions can be applied to users of *P2P* networks (i.e. to hosts on which clients of such networks are run):

- *Blocking options* — it is possible to block access to the Internet for a particular host or to restrict the access only to selected services (e.g. web and e-mail),
- *Bandwidth limitation* — it is possible to decrease speed of data transmission of *P2P* clients so that other users are not affected by too much data transferred by the line.

P2P Eliminator Configuration

P2P networks are detected automatically (the *P2P Eliminator* module keeps running). To set the *P2P Eliminator* module's parameters, go to the *P2P Eliminator* tab in the *Configuration* → *Advanced Options* section.

[5] According to thorough tests, the detection is highly reliable (probability of failure is very low).

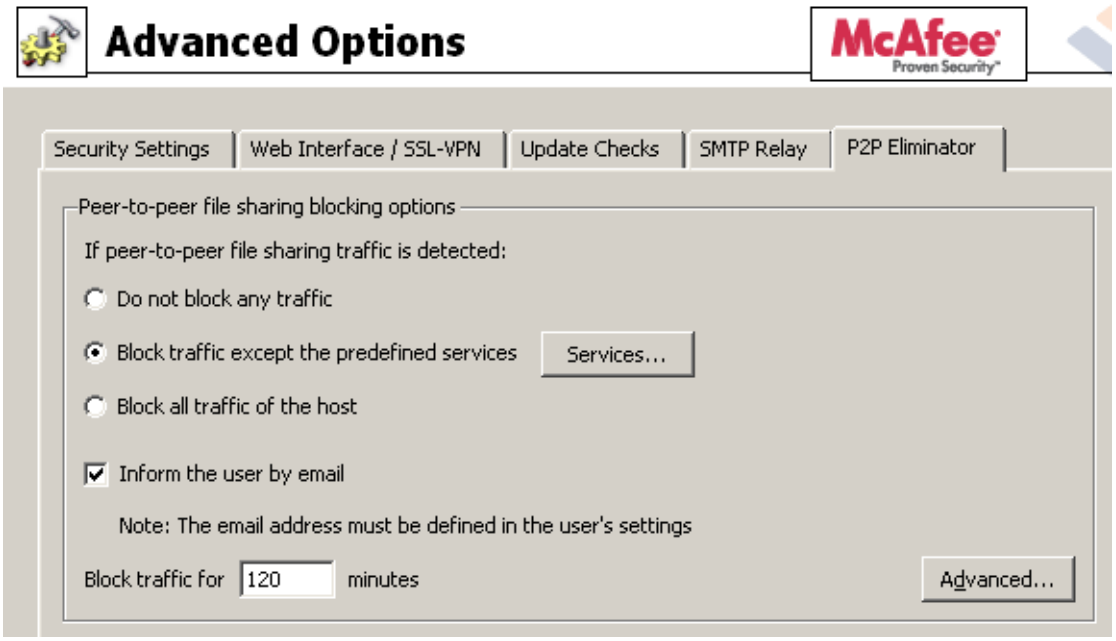


Figure 15.1 Detection settings and P2P Eliminator

As implied by the previous description, it is not possible to block connections to particular *P2P* networks. *P2P Eliminator* enables to block connection to the Internet from particular hosts (*Block all traffic for the particular user*), to allow these users to connect to certain services only *Allow only predefined services*) or to set limit for the bandwidth (set speed limit) that can be used by *P2P* traffic. The settings will be applied to all clients of *P2P* networks detected by *P2P Eliminator*.

Use the *Services* button to open a dialog where services which will be allowed can be specified. All services defined in *Configuration* → *Definitions* → *Services* are available (for details, refer to chapter 12.3).

Check the *Inform user by email* option if you wish that users at whose hosts *P2P* networks are detected will be warned and informed about actions to be taken (blocking of all traffic / time-limited restrictions for certain services and length of the period for which restrictions will be applied). The email is sent only if a valid email address (see chapter 13.1) is specified in the particular user account. This option does not apply to unauthenticated users.

Use the *Block traffic for ... minutes* parameter to specify the length of time during which traffic will be blocked for the particular host. The *P2P Eliminator* module enables traffic for this user automatically when the specified time expires. The time of disconnection should be long enough to make the user consider consequences and to stop trying to connect to *P2P* networks.

If traffic of *P2P* network clients is not blocked, it is possible to set bandwidth limitation for *P2P* networks at the bottom of the *P2P Eliminator* tab. Internet lines are usually asymetric (the speed vary for incoming and outgoing direction); therefore, this limitation is set separately for each direction. Bandwidth limitation applies only to traffic of *P2P* networks, other services are not affected.

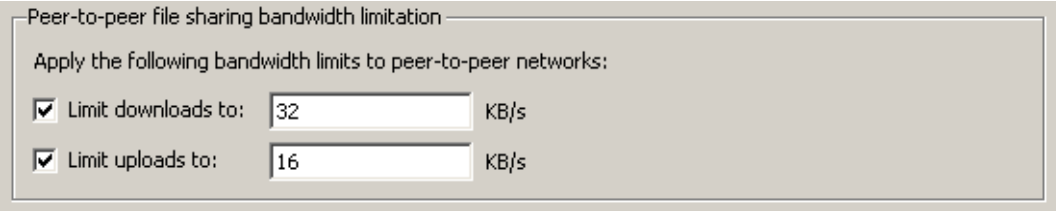


Figure 15.2 Bandwidth limits applied to P2P networks

Notes:

1. If a user who is allowed to use *P2P* networks (see chapter 13.1) is connected to the firewall from a certain host, no *P2P* restrictions are applied to this host. Settings in the *P2P Eliminator* tab are always applied to unauthorized users.

2. Information about *P2P* detection and blocked traffic can be viewed in the *Status* → *Hosts / users* section (for details, refer to chapter 17.1).

3. If you wish to notify also another person when a *P2P* network is detected (e.g. the *WinRoute* administrator), define the alert on the *Alerts Settings* tab of the *Configuration* → *Accounting* section. For details, see chapter 17.3.

Parameters for detection of P2P networks

Click *Advanced* to set parameters for *P2P* detection:

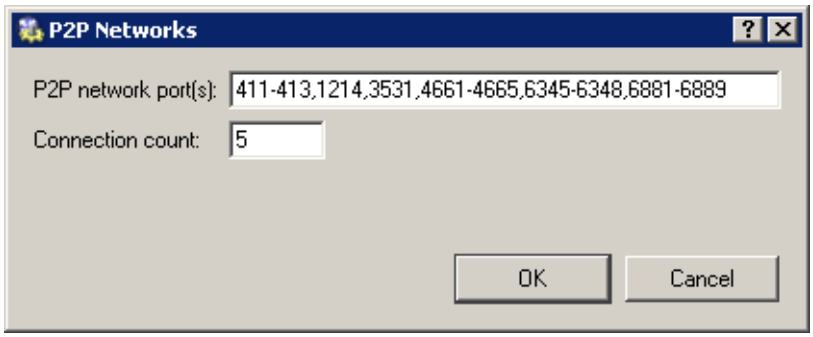


Figure 15.3 Settings of P2P networks detection

- *P2P network port(s)* — list of ports which are exclusively used by *P2P* networks. These ports are usually ports for control connections — ports (port ranges) for data sharing can be set by users themselves.

  You can use the *P2P network port(s)* entry to specify ports or port ranges. Use comas to separate individual values.

- *Connection count* — minimal number of concurrent connections which the user must reach to run *P2P* networks detection.

  Big volume of established connections is a typical feature of *P2P* networks (usually one connection for each file).

  The optimum value depends on circumstances (type of user's work, frequently used network applications, etc.) and it must be tested. If the value is too low, the system can be unreliable (users who do not use *P2P* networks might be suspected). If the value is too high, reliability of the detection is decreased (less *P2P* networks are detected).

15.2 Special Security Settings

WinRoute provides several security options which cannot be defined by traffic rules. These options can be set in the *Security settings* tab of the *Configuration* → *Advanced Options* section.

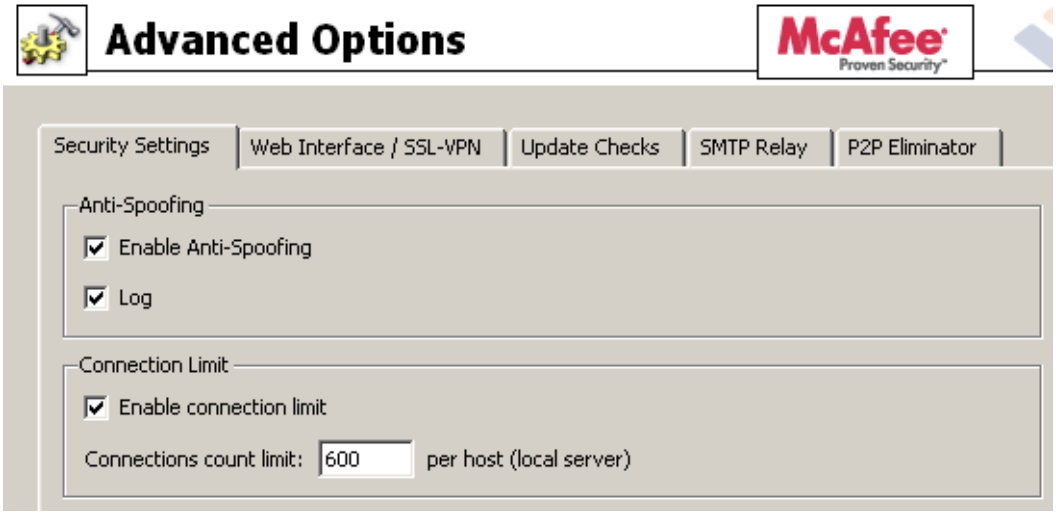


Figure 15.4 Security options — Anti-Spoofing and cutting down number of connections for one host

Anti-Spoofing

Anti-Spoofing checks whether only packets with allowed source IP addresses are received at individual interfaces of the *WinRoute* host. This function protects *WinRoute* host from attacks from the internal network that use false IP addresses (so called *spoofing*).

For each interface, any source IP address belonging to any network connected to the interface is correct (either directly or using other routers). For any interface connected to the Internet (so called external interface), any IP address which is not allowed at any other interface is correct.

Detailed information on networks connected to individual interfaces is acquired in the routing table.

The *Anti-Spoofing* function can be configured in the *Anti-Spoofing* folder in *Configuration / Advanced Options*.

Enable Anti-Spoofing
: This option activates *Anti-Spoofing*.

Log
: If this option is on, all packets that have not passed the anti-spoofing rules will be logged in the *Security* log (for details see chapter 20.11).

Connections Count Limit

This function defines a limit for the maximum number of connections per a local host. This function can be enabled/disabled and set through the *Security Settings* tab in *Configuration → Advanced Options*.

This function can be helpful especially for the following cases:

- Any service (e.g. WWW server) which is available from the Internet (allowed by traffic rules —see chapter 6) is running on the local network. Connection count limits protect internal servers from flooding (*DoS* type attacks — *Denial of Service*).

  In this case, the limit is applied to the local server — sum of all connections of all connected clients must not exceed this limit.

- Client computer (workstation) in the local network is attacked by a worm or a Trojan horse which is trying to establish a connection to many servers. Connection count limits protects the *WinRoute* host from flooding and it can reduce undesirable activities by worms and Trojan horses.

  In this case, the limit is applied to a host (workstation) in the local network — the sum of all connections established from this computer to individual servers in the Internet must not exceed the limit.

15.3 VPN using IPSec Protocol

IPsec (*IP Security Protocol*) is an extended IP protocol which enables secure data transfer. It provides services similar to SSL/TLS, however, these services are provided on a network layer. *IPSec* can be used for creation of encrypted tunnels between networks (VPN) — so called tunnel mode, or for encryption of traffic between two hosts— so called transport mode.

WinRoute includes so called *IPSec* pass-through. This implies that *WinRoute* does not include tools for establishing an *IPSec* connection (tunnel), however, it is able to detect *IPSec* protocol and enable it for traffic between the local network and the Internet.

Note: The *IPSec* Pass-Through function guarantees full functionality of existing *IPSec* clients and servers after deployment of *WinRoute* at the Internet gateway. If you consider designing and implementation of new virtual private networks, we recommend you to use the *WinRoute* proprietary VPN solution (see chapter 21).

IPSec preferences

IPSec preferences can be set in the *IPSec pass-through* area in the *Security Settings* tab of the *Configuration* → *Advanced Options* section. For detailed information on IPSec refer to chapter *WinRoute's IPSec configuration*.

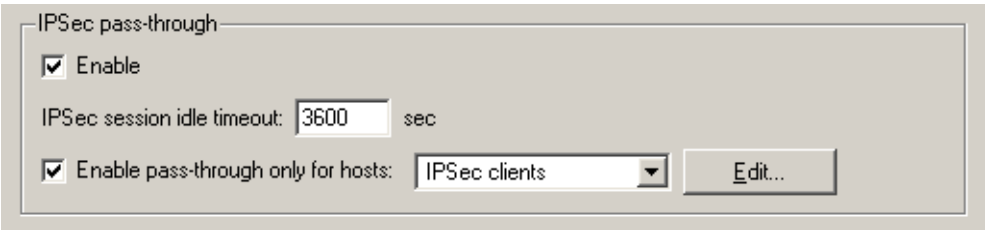


Figure 15.5 IPSec pass-through settings (the Security Settings tab under Configuration → Advanced Options)

Enable

This option enables *IPSec* pass-through.

It is necessary to set idle timeout for *IPSec* connections (default time is 3600 seconds which is exactly 1 hour). If no data is transferred for this time and a connection is not closed properly, *WinRoute* will consider the connection closed and the pass-through is available to another computer (another IP address).

Enable pass-through only for hosts

It is possible to narrow the number of hosts using *IPSec* pass-through by defining a certain scope of IP addresses (typically hosts on which IPSec clients will be run). Use the *Edit* button to edit a selected IP group or to add a new one.

WinRoute's IPSec configuration

Generally, communication through *IPSec* must be permitted by firewall policy (for details refer to chapter 6.3). IPSec protocol uses two traffic channels:

- *IKE* (*Internet Key Exchange* — exchange of encryption keys and other information). IKE
- encrypted data (*IP* protocol number 50 is used)

Open the *Configuration* → *Traffic Policy* section to define a rule which will permit communication between IPSec clients (VPN address group is described in the example) and IPSec server for the services (`ipsec.server.cz` server is described in the example).

Figure 15.6 Enabling IPSec by a traffic rule

Note: Predefined *IPSec* and *IKE* services are provided in *WinRoute*.

IPSec client in local network

This section of the guide describes *WinRoute* configuration for cases when an IPSec client or the server is located in the local network and *WinRoute* provides translation of IP addresses (NAT — for details see chapter 6).

1. *IPSec client on WinRoute host*

   In this case IPSec traffic is not influenced by NAT (IPSec client must be set so that it uses the public IP address of the *WinRoute* host). It is only necessary to define a traffic rule permitting IPSec communication between the firewall and the IPSec server.

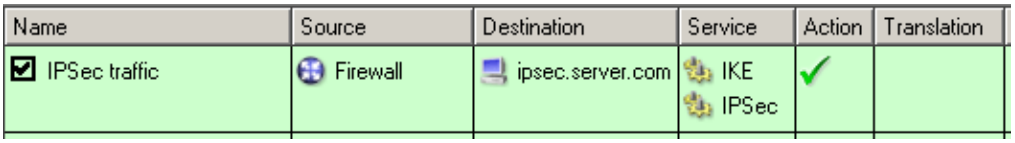


Figure 15.7 Traffic rule for IPSec client on the WinRoute host

The *Translation* column must be blank — no IP translation is performed. The pass-through setting is not important in this case (it cannot be applied).

2. One IPSec client in the local network (one tunnel)

   If only one IPSec tunnel from the local network to the Internet is created at one moment, then it depends on the type of IPSec client:

   - If IPSec client and the IPSec server support the *NAT Traversal* function (the client and the server are able to detect that the IP address is translated on the way between them), IPSec must be *disabled* (otherwise a collision might arise).

     NAT Traversal is supported for example by *Nortel Networks'* VPN software (`http://www.nortelnetworks.com/`).

   - If the IPSec client does not support *NAT Traversal*, it is necessary to *enable* IPSec pass-through in *WinRoute*.

   In both cases, IPSec communication between the client and the IPSec server must be permitted by a traffic rule. NAT must be defined in the *Translation* column (in the same way as for the communication from the local network to the Internet).

Name	Source	Destination	Service	Action	Translation
IPSec client -> server	192.168.1.110	ipsec.server.com	IKE IPSec	✓	NAT (Default outgoing interface)

Figure 15.8 Traffic rule for one IPSec client in the local network

3. *Multiple IPSec clients in the local network (multiple tunnels)*

   If multiple IPSec tunnels from the local network to the Internet are supposed to be created, all IPSec clients and corresponding servers must support *NAT Traversal* (see above). Support for IPSec in *WinRoute* must be *disabled* so that no collisions arise.

   Again, traffic between the local network and corresponding IPSec servers must be permitted by a traffic rule.

Name	Source	Destination	Service	Action	Translation
IPSec clients -> servers	IPSec clients	ipsec.server.com	IKE IPSec	✓	NAT (Default outgoing interface)

Figure 15.9 Traffic rule for multiple IPSec clients in the local network

IPSec server in local network

An IPSec server on a host in the local network or on the *WinRoute* host must be mapped from the Internet. In this case, traffic between Internet clients and the *WinRoute* host must be permitted by a traffic rule and mapping to a corresponding host in the local network must be set.

Warning: Only a single IPSec server can be mapped from the public IP address of the firewall. For mapping of multiple IPSec servers, the firewall must use multiple public IP addresses.

Example: We want to set that two IPSec servers will be available from the Internet — one on the *WinRoute* host and another on a host with the IP address `192.168.100.100`. The firewall interface connected to the Internet uses IP addresses `60.80.100.120` and `60.80.100.121`.

Name	Source	Destination	Service	Action	Translation
IPSec server #1	Clients of server #1	60.80.100.120	IKE IPSec	✓	
IPSec server #2	Clients of server #2	60.80.100.121	IKE IPSec	✓	MAP 192.168.1.50

Figure 15.10 Traffic rules for two IPSec servers

Chapter 16

Other settings

16.1 Routing table

Using *Administration Console* you can view or edit the system routing table of the host where *WinRoute* is running. This can be useful especially to resolve routing problems remotely (it is not necessary to use applications for terminal access, remote desktop, etc.).

To view or modify the routing table go to *Configuration* → *Routing Table*. This section provides up-to-date version of the routing table of the operating system including so called *persistent routes* (routes added by the `route -p` command).

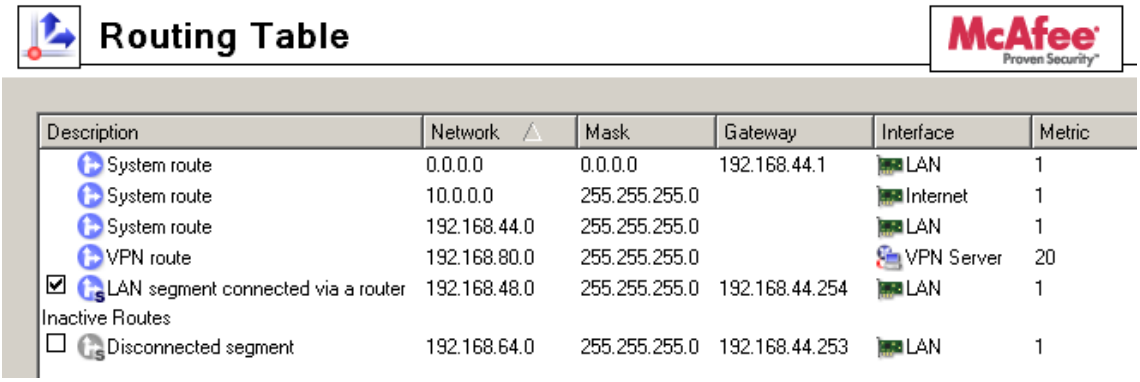


Figure 16.1 Firewall's system routing table

Dynamic and static routes can be added/removed in this section. Dynamic routes are valid only until the operating system is restarted or until removed by the `route` system command. Static routes are saved in *WinRoute* and they are restored upon each restart of the operating system.

Warning: Changes in the routing table might interrupt the connection between the *WinRoute Firewall Engine* and the *Administration Console*. We recommend to check the routing table thoroughly before clicking the *Apply* button!

Route Types

The following route types are used in the *WinRoute* routing table:

- *System routes* — routes downloaded from the operating system's routing table (including so called persistent routes). These routes cannot be edited some of them can be removed — see the *Removing routes from the Routing Table* section).

- *Static routes* — manually defined routes managed by *WinRoute* (see below). These routes can be added, modified and/or removed.

  The checking boxes can be used to disable routes temporarily —such routes are provided in the list of inactive routes. Static routes are marked with an *S* icon.

- *VPN routes* — routes to VPN clients and to networks at remote endpoints of VPN tunnels (for details, see chapter 21). These routes are created and removed dynamically upon connecting and disconnecting of VPN clients or upon creating and removing of VPN tunnels. VPN routes cannot be created, modified nor removed by hand.

- *Inactive routes* — routes which are currently inactive are showed in a separate section. These can be static routes that are temporarily disabled, static routes via an interfaces which has been disconnected or removed from the system, etc.

Static routes

WinRoute includes a special system for creation and management of static routes in the routing table. All static routes defined in *WinRoute* are saved into the configuration file and upon each startup of the *WinRoute Firewall Engine* they are added to the system routing table. In addition to this, these routes are monitored and managed all the time *WinRoute* is running. This means that whenever any of these routes is removed by the `route` command, it is automatically added again.

Notes:

1. The operating system's persistent routes are not used for implementation of static routes (for management of these routes, *WinRoute* uses a proprietary method).

2. If a static connection uses a dial-up, any UDP or TCP packet with the *SYN* flag dials the line. For detailed information, see chapter 16.2.

Definitions of Dynamic and Static Rules

Click on the *Add* (or *Edit* when a particular route is selected) button to display a dialog for route definition.

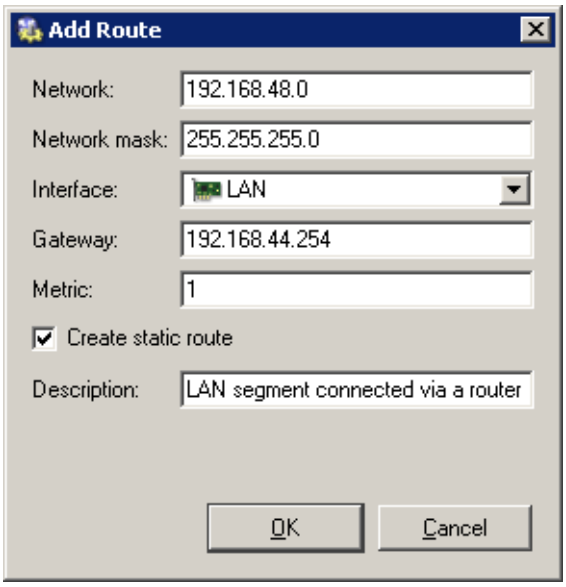


Figure 16.2 Adding a route to the routing table

Network, Network Mask
: IP address and mask of the destination network.

Interface
: Selection of an interface through which the specific packet should be forwarded.

Gateway
: IP address of the gateway (router) which can route to the destination network. The IP address of the gateway must be in the same IP subnet as the selected interface.

Metric
: "Distance" of the destination network. The number stands for the number of routers that a packet must pass through to reach the destination network.
Metric is used to find the best route to the desired network. The lower the metric value, the "shorter" the route is.
Note: Metric in the routing table may differ from the real network topology. It may be modified according to the priority of each line, etc.

Create a static route
: Enable this option to make this route static. Such route will be restored automatically by *WinRoute*(see above). A brief description providing various information (why the route was created, etc.) about the route can be attached.

If this option is not enabled, the route will be valid only until the operating system is restarted or until removed manually in the *Administration Console* or using the `route` command.

Removing routes from the Routing Table

Using the *Remove* button in the *WinRoute* admin console, records can be removed from the routing table. The following rules are used for route removal:

- Static routes in the *Static Routes* folder are managed by *WinRoute*. Removal of any of the static routes would remove the route from the system routing table immediately and permanently (after clicking on the *Apply* button).
- Dynamic (system) route will be removed as well, regardless whether it was added in the *Administration Console* or by the `route` command. However, it is not possible to remove any route to a network which is connected to an interface.
- Persistent route of the operating system will be removed from the routing table only after restart of the operating system. Upon reboot of the operating system, it will be restored automatically. There are many methods that can be used to create persistent routes (the methods vary according to operating system — in some systems, the `route -p` command can be used, etc.). It is not possible to find out how a particular persistent route was created and how it might be removed for good.

16.2 Demand Dial

If the *WinRoute* host is connected to the Internet via dial-up, *WinRoute* can automatically dial the connection when users attempt to access the Internet. *WinRoute* provides the following options of dialing/hanging control:

- Line is dialed when a request from the local network is received. This function is called Demand dial. For further description see below.
- Line is disconnected automatically if idle for a certain period (no data is transmitted in both directions). For a description of the automatic disconnection, refer to chapter 5.1.

How demand dial works

First, the function of demand dial must be activated within the appropriate line (either permanently or during a defined time period). This may be defined in *Configuration* → *Interfaces* (for details see chapter 5.1).

Second, there must be no default gateway in the operating system (no default gateway must be defined for any network adapter). This condition does not apply to the dial-up line which is used for the Internet connection — this line will be configured in accordance with information provided by the ISP.

If *WinRoute* receives a packet from the local network, it will compare it with the system routing table. If the packets goes out to the Internet, no record will be found, since there is no default route in the routing table. Under usual circumstances, the packet would be dropped and a control message informing about unavailability of the target would be sent to the sender. If no default route is available, *WinRoute* holds the packet in the cache and dials the appropriate line if the demand dial function is enabled. This creates an outgoing route in the routing table via which the packet will be sent.

To avoid undesired dialing of the line, line dialing is allowed by certain packet types only. The line can be dialed only by UDP or TCP packets with the *SYN* flag (connection attempts). Demand dialing is disabled for *Microsoft Networks* services (sharing of files and printers, etc.).

Since this moment, the default route exists and other packets directed to the Internet will be routed via a corresponding line. The line may be either disconnected manually or automatically if idle for a certain time period. When the line is hung-up, the default route is removed from the routing table. Any other packet directed to the Internet redials the line.

Notes:

1. To ensure correct functionality of demand dialing there must be no default gateway set at network adapters. If there is a default gateway at any interface, packets to the Internet would be routed via this interface (no matter where it is actually connected to) and *WinRoute* would not dial the line.

2. If multiple demand dial RAS lines are defined in *WinRoute*, the one that was defined first will be used. *WinRoute* does not enable automatic selection of a line to be dialed.

3. Lines can be also dialed if this is defined by a static route in the routing table (refer to chapter 16.1). If a static route via the dial-up is defined, the packet matching this route will dial the line. This line will not be used as the default route — the *Use default gateway on remote network* option in the dial-up definition will be ignored.

4. According to the factors that affect total time since receiving the request until the line is dialed (i.e. line speed, time needed to dial the line, etc.) the client might consider the destination server unavailable (if the timeout expires) before a successful connection attempt. However, *WinRoute* always finishes dial attempts. In such cases, simply repeat the request, i.e. with the *Refresh* button in your browser.

Technical Peculiarities and Limitations

Demand dialing has its peculiarities and limitations. The limitations should be considered especially within designing and configuration of the network that will use *WinRoute* for connection and of the dial-up connected to the Internet.

1. Demand dial cannot be performed directly from the host where *WinRoute* is installed because it is initiated by *WinRoute* low-lever driver. This driver holds packets and decides whether the line should be dialed or not. If the line is disconnected and a packet is sent from the local host to the Internet, the packet will be dropped by the operating system before the *WinRoute* driver is able to capture it.

2. Typically the server is represented by the DNS name within traffic between clients and an Internet server. Therefore, the first packet sent by a client is represented by the DNS query that is intended to resolve a host name to an IP address.

   In this example, the DNS server is the *WinRoute* host (this is very common) and the line to the Internet is disconnected. A client's request on this DNS server is traffic within the local network and, therefore, it will not result in dialing the line. If the DNS server does not have the appropriate entry in the cache , it must forward the request to another server on the Internet. The packet is forwarded to the Internet by the local DNS client that is run at the *WinRoute* host. This packet cannot be held and it will not cause dialing of the line. Therefore, the DNS request cannot be answered and the traffic cannot continue.

   For these reasons, *WinRoute DNS Forwarder* enables automatic dialing (if the DNS server cannot respond to the request itself). This function is dependent on demand dial — if the demand dial function is disabled, the *DNS Forwarder* will not dial the line.

   Note: If the DNS server is located on another host within the local network or clients within the local network use an Internet DNS server, then the limitation is irrelevant and the dialing will be available. If clients' DNS server is located on the Internet, the line will be dialed upon a client's DNS query. If a local DNS server is used, the line will be dialed upon a query sent by this server to the Internet (the default gateway of the host where the DNS server is running must be set to the IP address of the *WinRoute* host).

3. It can be easily understood through the last point that if the DNS server is to be running at the *WinRoute* host, it must be represented by *DNS Forwarder* because it can dial the line if necessary.

   If there is a domain that is based on Active Directory in the Windows 2000 local network, Microsoft DNS server must be used as communication with Active Directory

is performed according to special types of DNS requests. Microsoft DNS server does not support automatic dialing. Moreover, it cannot be used at the same host as *DNS Forwarder* as it would cause collision of ports.

As understood from the facts above, if the Internet connection is to be available via dial-up, *WinRoute cannot* be used at the same host where Windows 2000 server Active Directory and Microsoft DNS are running.

4. If *DNS Forwarder* is used, *WinRoute* can dial as a response to a client's request if the following conditions are met:

   - Destination server must be defined by DNS name so that the application can create a DNS query.
   - In the operating system, set the primary DNS server to the IP address of the firewall). In Windows operating system, go to TCP/IP properties and set the IP address of this interface as the primary DNS.
   - *DNS Forwarder* must be configured to forward requests to one of the defined DNS servers (the *Forward queries to the specified DNS server(s)* option). Automatic detection of DNS servers are not available. For details, refer to chapter 5.3.

5. The *Proxy server* in *WinRoute* (see chapter 5.5) also provides direct dial-up connections. A special page providing information on the connection process is opened (the page is refreshed in short periods). Upon a successful connection, the browser is redirected to the specified Website.

Setting Rules for Demand Dial

Demand dial functions may cause unintentional dialing. It's usually caused by DNS queries that are handled by the *DNS Forwarder* The following causes apply:

- User host generates a DNS query in the absence of the user. This traffic attempt may be an active object at a local HTML page or automatic update of an installed application.
- *DNS Forwarder* performs dialing in response to requests of names of local hosts. Define DNS for the local domain properly (use the `hosts` system file of the *WinRoute* host — for details see chapter 5.3).

Note: In *WinRoute*, unwanted traffic may be blocked. However, for security reasons it is recommended to detect the root of the problem (i.e. use antivirus to secure the workstation, etc.).

In *Configuration* → *Demand Dial* within *Administration Console*, rules for dialing certain DNS names may be defined.

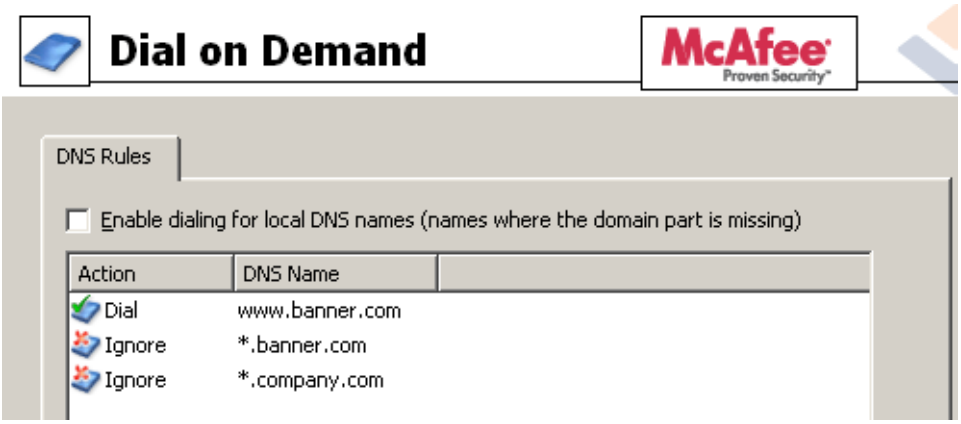


Figure 16.3 Demand dial rules (for responses to DNS queries)

In this section you can create a rule list of DNS names.

Either whole *DNS name* or only its end or beginning completed by an asterisk (*) may be entered. An asterisk may stand for any number of characters.

In *Actions* you can select from the *Dial* or *Ignore* options. Use the second option to block dialing of the line in response to a query on the DNS name.

Rule lists are searched downwards (rule order can be modified with the arrows at the right side of the window). When the system detects the first rule that meets all requirements, the desired action is executed and the search is stopped. All DNS names missing a suitable rule will be dialed automatically by *DNS Forwarder* when demanded.

The *Dial* action can be used to create complex rule combinations. For example, dial can be permitted for one name within the domain and denied for the others (see the figure).

Dial of local DNS names

Local DNS names are names of hosts within the domain (names that do not include a domain).

Example: The local domain is called `company.com`. The host is called `pc1`. The full name of the host is `pc1.company.com` whereas local name in this domain is `pc1`.

Local names are usually stored in the database of the local DNS server (in this example, the names are stored in the `hosts` file at the *WinRoute* host that uses *DNS Forwarder*). Set by default, *DNS Forwarder* does not dial these names as names are considered non-existent unless they can be found in the local DNS database.

If the primary server of the local domain is located outside of the local network, it is necessary that the *DNS Forwarder* also dials the line if requests come from these names. Activate the *Enable dialing for local DNS names* option in the *Other settings* tab to enable this (at the top of the *Demand Dial* dialog window). In other cases, it is recommended to leave the option disabled (again, the line can be dialed undesirably).

16.3 Universal Plug-and-Play (UPnP)

WinRoute supports UPnP protocol (*Universal Plug-and-Play*). This protocol enables client applications (i.e. *Microsoft MSN Messenger*) to detect the firewall and make a request for mapping of appropriate ports from the Internet for the particular host in the local network. Such mapping is always temporary — it is either applied until ports are released by the application (using UPnP reports) or until expiration of the timeout.

The required port must not collide with any existing mapped port or any traffic rule allowing access to the firewall from the Internet. Otherwise, the UPnP port mapping request will be denied.

Configuration of the UPnP support

To configure UPnP go to the *Security Settings* folder in *Configuration* → *Advanced Options*.

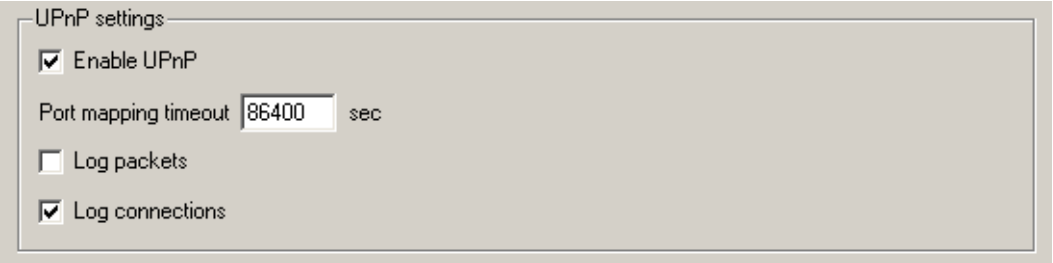


Figure 16.4 IPnP settings (the Security Settings tab under Configuration / Advanced Options)

Enable UPnP

This option enables UPnP.

Warning: If *WinRoute* is running on the Windows XP operating system, check whether the following system services are not running before you start the *UPnP* function:

- *SSDP Discovery Service*
- *Universal Plug and Play Device Host*

If any of these services is running, close it and deny its automatic startup. In *WinRoute* these services cannot be used together with *UPnP*.

Note: The *WinRoute* installation program detects the services and offers their stopping and denial.

Port mapping timeout

For security reasons, ports required by applications are mapped for a certain time period only. Mapping is closed automatically on demand of the application or when the timeout (in seconds) expires.

UPnP also enables the application to open ports for a requested period. Here the *Port mapping timeout* parameter also represents a maximal time period that the port will be available to an application (even if the application demands a longer period, the period is automatically reduced to this value).

Log packets
If this option is enabled, all packets passing through ports mapped with UPnP will be recorded in the *Security* log (see chapter 20.11)).

Log connections
If this option is enabled, all packets passing through ports mapped with UPnP will be recorded in the *Connection* log (see chapter 20.5).

Warning: Apart from the fact that UPnP is a useful feature, it may also endanger network security, especially in case of networks with many users where the firewall could be controlled by too many users. A *WinRoute* administrator should consider carefully whether to prefer security or functionality of applications that require UPnP.

Using traffic policy (see chapter 6.3) you can limit usage of UPnP and enable it to certain IP addresses or certain users only.

Example:

Name	Source	Destination	Service	Action	Translation
Allow UPnP for selected hosts	UPnP clients	Firewall	UPnP	✓	
Deny UPnP	LAN	Firewall	UPnP	✗	

Figure 16.5 Traffic rules allowing UPnP for specific hosts

The first rule allows UPnP only from *UPnP Clients* IP group. The second rule denies UPnP from other hosts (IP addresses).

16.4 Relay SMTP server

WinRoute provides a function which enables notification to users or/and administrators by email alerts. These alert messages can be sent upon various events, for example when a virus is detected (see chapter 11.3), when a *Peer-to-Peer* network is detected (refer to chapter 15.1), when an alert function is set for certain events (details in chapter 13.1) or upon reception of an alert (see chapter 17.3).

For this purpose, *WinRoute* needs an SMTP Relay Server. This server is used for forwarding of infected messages to a specified address.

Note: WinRoute does not provided any built-in SMTP server.

To configure an SMTP server, go to the *SMTP server* tab in *Configuration* → *Advanced Options*.

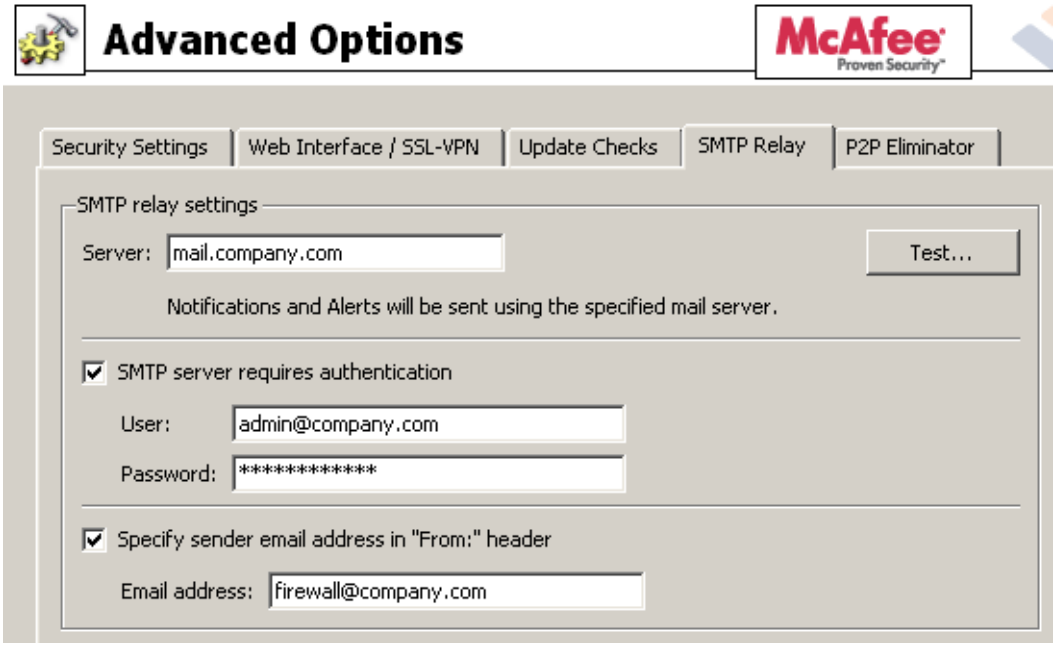


Figure 16.6 SMTP settings — reports sending

Server

Name or IP address of the server.

Note: If available, we recommend you to use an SMTP server within the local network (messages sent by *WinRoute* are often addressed to local users).

SMTP requires authentication

Enable this option to require authentication through username and password at the specified SMTP server.

Specify sender email address in "From" header

In this option you can specify a sender's email address (i.e. the value for the `From` header) for email sent from *WinRoute* (email or SMS alerts sent to users). Preset `From` header does not apply to messages forwarded during antivirus check (refer to chapter 11.4).

This item must be preset especially if the SMTP server strictly checks the header (messages without or with an invalid `From` header are considered as spams). The item can also be used for reference in recipient's mail client or for email classification. This is why it is always recommended to specify sender's email address in *WinRoute*.

Test

Click *Test* to test functionality of sending of email via the specified SMTP server. *WinRoute* sends a testing email message to the specified email address.

Warning:

1. If SMTP is specified by a DNS name, it cannot be used until *WinRoute* resolves a corresponding IP address (by a DNS query). The *IP address of specified SMTP server cannot be resolved* warning message is displayed in the *SMTP Relay* tab until the IP address is not found. If the warning is still displayed, this implies that an invalid (non-existent) DNS name is specified or the DNS server does not respond.

   If the warning on the *SMTP server* tab is still displayed, it means that an invalid DNS name was specified or that an error occured in the communication (DNS server is not responding). Therefore, we recommend you to specify SMTP server by an IP address if possible.

2. Communication with the SMTP server must not be blocked by any rule, otherwise the *Connection to SMTP server is blocked by traffic rules* error is reported upon clicking the *Apply* button.

   For detailed information about traffic rules, refer to chapter 6.

Chapter 17

Status Information

WinRoute activities can be well monitored by the administrator (or by other users with appropriate rights). There are three types of information — status monitoring, statistics and logs.

- Communication of each computer, users connected or all connections using *WinRoute* can be monitored.

  Notes:

  1. *WinRoute* monitors only traffic between the local network and the Internet. The traffic within the local network is not monitored.

  2. Only traffic allowed by traffic rules (see chapter 6) can be viewed. If a traffic attempt which should have been denied is detected, the rules are not well defined.

- Statistics provide information on users and network traffic for a certain time period. Statistics are viewed in the form of charts and tables. For details see chapter 18.

- Logs are files where information about certain activity is reported (e.g. error or warning reports, debug information etc.). Each item is represented by one row starting with a timestamp (date and time of the event). In all language versions of *WinRoute*, reports recorded are available in English only and they are generated by the *WinRoute Firewall Engine*. For details, refer to chapter 20.

The following chapters describe what information can be viewed and how its viewing can be changed to accommodate the user's needs.

17.1 Active hosts and connected users

In *Status* → *Active Hosts*, the hosts within the local network or active users using *WinRoute* for communication with the Internet will be displayed.

Note: For more details about the firewall user's logon see chapter 8.1.

Look at the upper window to view information on individual hosts, connected users, data size/speed, etc.

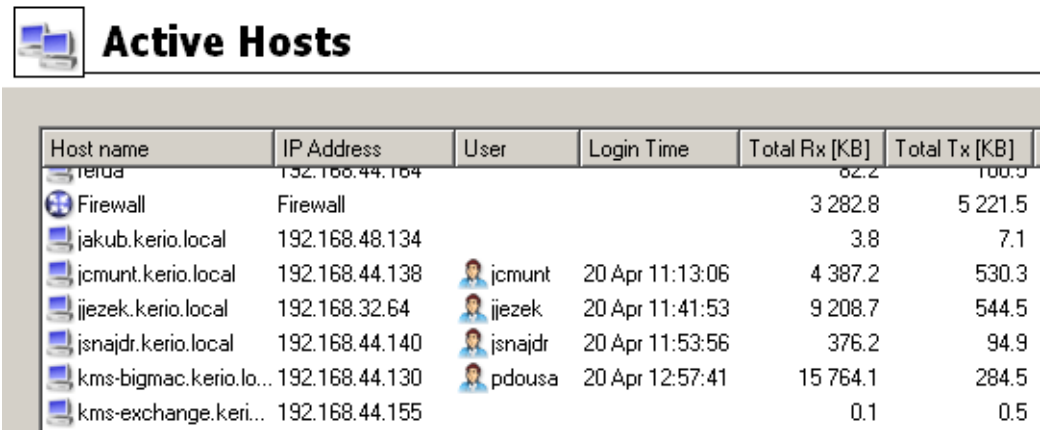


Figure 17.1 List of active hosts and users connected to the firewall

The following information can be found in the *Active Hosts* window:

Hostname
DNS name of a host. In case that no corresponding DNS record is found, IP address is displayed instead.

User
Name of the user which is connected from a particular host. If no user is connected, the item is empty.

Currently Rx, Currently Tx
Monitors current traffic speed (kilobytes per second) in both directions (from and to the host — *Rx* values represent incoming data, *Tx* values represent outgoing data)

The following columns are hidden by default. To view these columns select the *Modify columns* option in the context menu (see below).

IP address
IP address of the host from which the user is connecting from

Login time
Date and time of the recent user login to the firewall

Login duration
Monitors length of the connection. This information is derived from the current time status and the time when the user logged on

Inactivity time
Duration of the time with zero data traffic. You can set the firewall to logout users automatically after the inactivity exceeds allowed inactivity time (for more details see chapter 9.1)

Start time
Date and time when the host was first acknowledged by *WinRoute*. This information is kept in the operating system until the *WinRoute Firewall Engine* disconnected.

Total received, Total transmitted
Total size of the data (in kilobytes) received and transmitted since the *Start time*

Connections
Total number of connections to and from the host. Details can be displayed in the context menu (see below)

Authentication method
Authentication method used for the recent user connection:

- *plaintext* — user is connected through an insecure login site *plaintext*
- *SSL* — user is connected through a login site protected by SSL security system *SSL*
- *proxy* — a *WinRoute* proxy server is used for authentication and for connection to Websites
- *NTLM* — user was authenticated with NTLM in NT domain (this is the standard type of login if Microsoft Internet Explorer 5.5 or later or *Firefox/Netscape/Mozilla/SeaMonkey* core version 1.3 or later is used)
- *VPN client* — user has connected to the local network using the *Kerio VPN Client* (for details, see chapter 21).
  Note: Connections are not displayed and the volume of transmitted data is not monitored for VPN clients.

For more details about connecting and user authentication see chapter 8.1.

Information displayed in the *Active Hosts* window can be refreshed by clicking on the *Refresh*button.

Use the *Show / Hide details* to open the bottom window providing detailed information on a user, host and open connections.

Active Hosts dialog options

Clicking the right mouse button in the *Active Hosts* window (or on the record selected) will display a context menu that provides the following options:

User statistics
Use this option to switch to the *User statistics* tab in *Status* → *Statistics* where user statistics can be viewed.
This option is available only for hosts from which a user is connected at the moment.

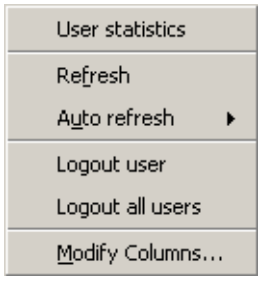


Figure 17.2 Context menu for the Active Hosts window

Refresh
This option refreshes information in the *Active Hosts* window immediately (this function is equal to the *Refresh* button displayed at the bottom of the window).

Auto refresh
Settings for automatic refreshing of the information in the *Active Hosts* window. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Logout user
Immediate logout of a selected user.

Logout all users
Immediate logout of all firewall users.

Manage Columns
By choosing this option you can select columns to be displayed in the *Active Hosts* window (see chapter 3.2).

Detailed information on a selected host and user

Detailed information on a selected host and connected user are provided in the bottom window of the *Active Hosts* section.

Open the *General* tab to view information on user's login, size/speed of transmitted data and information on activities of a particular user.

Login information
Information on logged-in users:

- *User* — name of a user, DNS name (if available) and IP address of the host from which the user is connected
- *Login time* — date and time when a user logged-in, authentication method that was used and inactivity time (idle).

If no user is connected from a particular host, detailed information on the host are provided instead of login information.

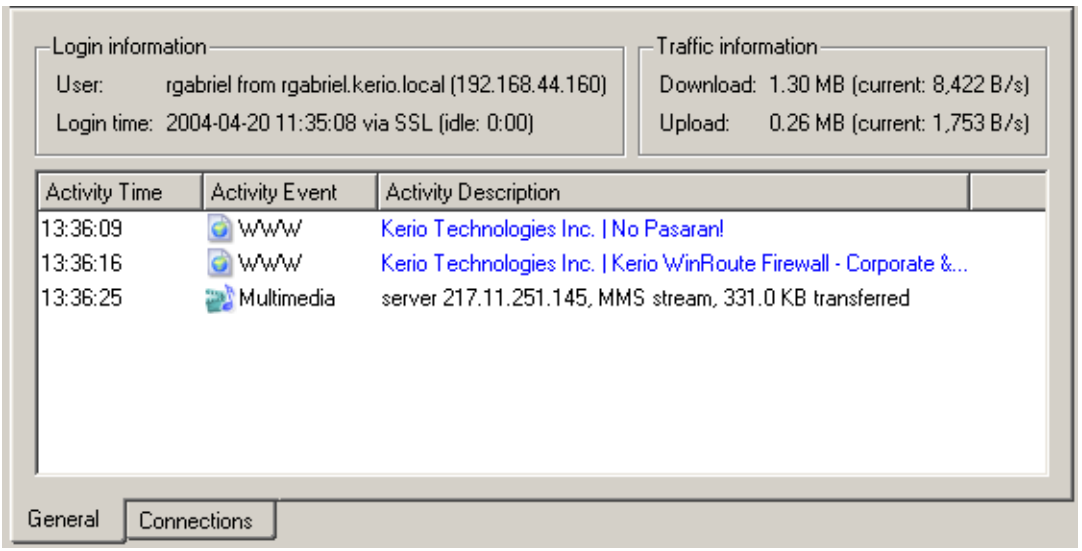

Login information
User: rgabriel from rgabriel.kerio.local (192.168.44.160)
Login time: 2004-04-20 11:35:08 via SSL (idle: 0:00)
Traffic information
Download: 1.30 MB (current: 8,422 B/s)
Upload: 0.26 MB (current: 1,753 B/s)
Activity Time
Activity Event
Activity Description
13:36:09 WWW Kerio Technologies Inc. | No Pasaran!
13:36:16 WWW Kerio Technologies Inc. | Kerio WinRoute Firewall - Corporate &...
13:36:25 Multimedia server 217.11.251.145, MMS stream, 331.0 KB transferred
General
Connections

Figure 17.3 Information about selected host/user — actions overview

Figure 17.4 Host info (if no user is connected from it)

- *Host* — DNS name (if available) and IP address of the host
- *Idle time* — time for which no network activity performed by the host has been detected

Traffic information

Information on size of data received (*Download*) and sent (*Upload*) by the particular user (or host) and on current speed of traffic in both directions.

Overview of detected activities of the particular user (host) are given in the main section of this window:

Activity Time

Time (in minutes and seconds) when the activity was detected.

Activity Event

Type of detected activity (network communication). *WinRoute* distinguishes between the following activities: *SMTP*, *POP3*, *WWW* (HTTP traffic), *FTP*, *Streams* (real-time transmission of audio and video streams) and *P2P* (use of Peer-to-Peer networks).

Note: WinRoute is not able to recognize which type of *P2P* network is used. According to results of certain testing it can only "guess" that it is possible that the client is connected to such network. For details, refer to chapter 15.1.

Activity Description

Detailed information on a particular activity:

- *WWW* — title of a Web page to which the user is connected (if no title is available, URL will be displayed instead). Page title is a hypertext link — click on this link to open a corresponding page in the browser which is set as default in the operating system.
- *SMTP, POP3* — DNS name or IP address of the server, size of downloaded/uploaded data.
- *FTP* — DNS name or IP address of the server, size of downloaded/saved data, information on currently downloaded/saved file (name of the file including the path, size of data downloaded/uploaded from/to this file).
- *Multimedia* (real time transmission of video and audio data) — DNS name or IP address of the server, type of used protocol (*MMS*, *RTSP*, *RealAudio*, etc.) and volume of downloaded data.
- *P2P* — information that the client is probably using Peer-To-Peer network.

Connections

The *Connections* tab provides detailed information on connections from and to a selected host. The list of connections provides an overview of services used by the selected user. Undesirable connections can be terminated immediately.

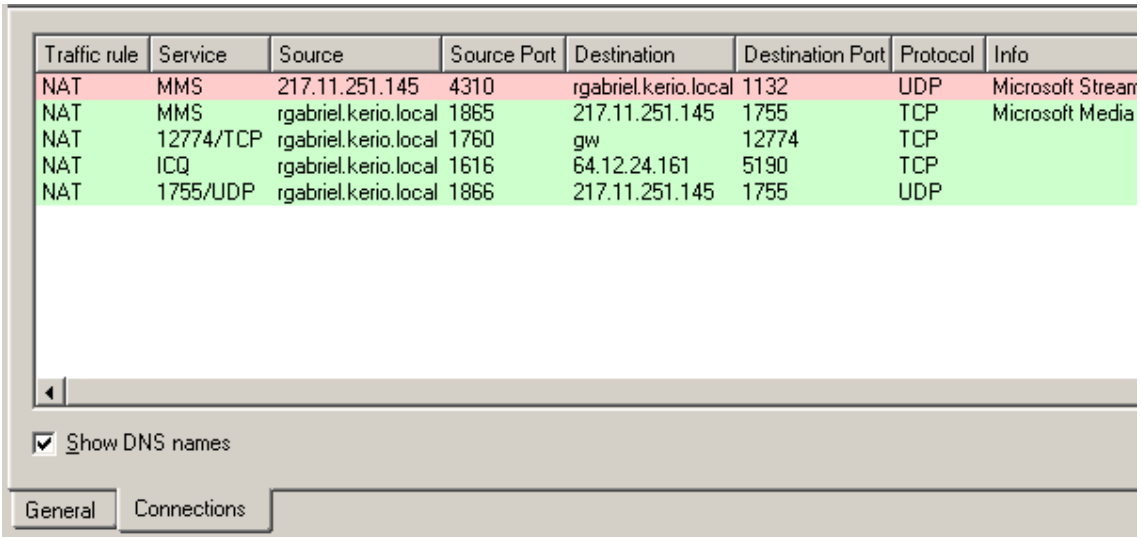


Figure 17.5 Information about selected host/user — connections overview

Information about connections:

Traffic rule
Name of the *WinRoute* traffic rule (see chapter 6) by which the connection was allowed.

Service
Name of the service. For non-standard services, port numbers and protocols are displayed.

Source, Destination
Source and destination IP address (or name of the host in case that the *Show DNS names* option is enabled —see below).

The following columns are hidden by default. They can be shown through the *Modify columns* dialog opened from the context menu (for details, see chapter 3.2).

Source port, Destination port
Source and destination port (only for TCP and UDP protocols).

Protocol
Protocol used for the transmission (TCP, UDP, etc.).

Timeout
Time left before the connection will be removed from the table of *WinRoute's* connections.
Each new packet within this connection sets timeout to the initial value. If no data is transmitted via a particular connection, *WinRoute* removes the connection from the table upon the timeout expiration — the connection is closed and no other data can be transmitted through it.

Rx, Tx
Volume of incoming (*Rx*) and outgoing (Tx) data transmitted through a particular connection (in KB).

Info
Additional information (such as a method and URL in case of HTTP protocol).

Use the *Show DNS names* option to enable/disable showing of DNS names instead of IP addresses in the *Source* and *Destination* columns. If a DNS name for an IP address cannot be resolved, the IP address is displayed.

You can click on the *Colors* button to open a dialog where colors used in this table can be set.

Note: Upon right-clicking on a connection, the context menu extended by the *Kill connection* option is displayed. This option can be used to kill the connection immediately.

Histogram

The *Histogram* tab provides information on data volume transferred from and to the selected host in a selected time period. The chart provides information on the load of this host's traffic on the Internet line through the day.

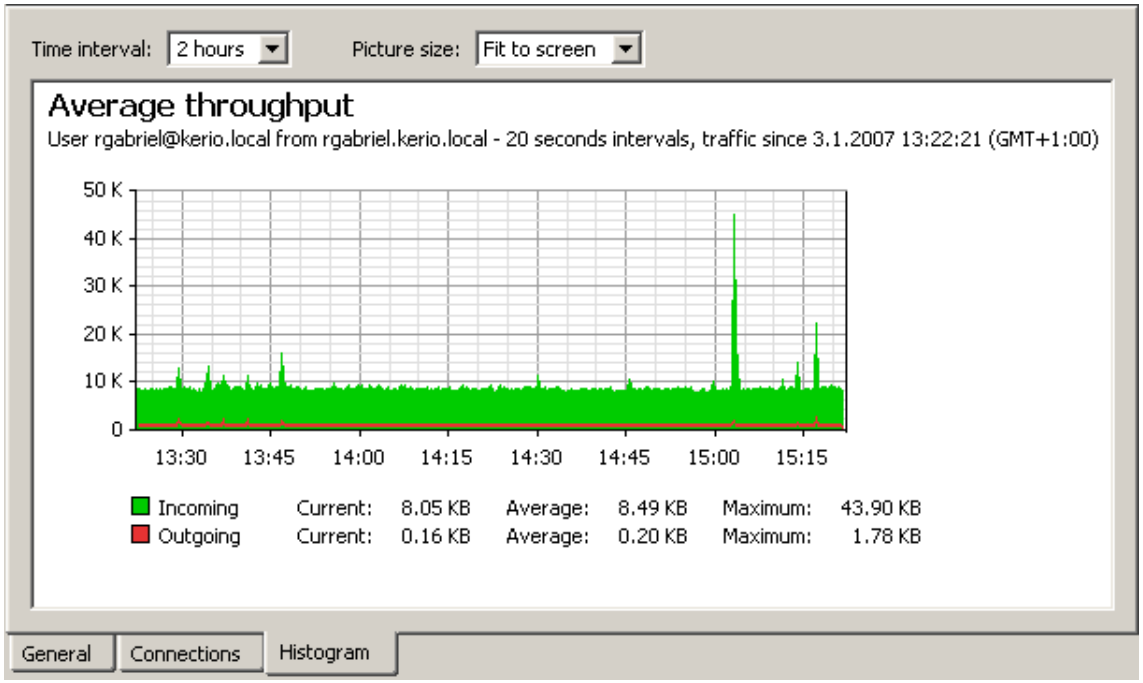


Figure 17.6 Information on selected host and user — traffic histogram

Select an item from the *Time interval* combo box to specify a time period which the chart will refer to (2 hours or 1 day). The x axis of the chart represents time and the y axis represents traffic speed. The x axis is measured accordingly to a selected time period, while measurement of the y axis depends on the maximal value of the time interval and is set automatically (bytes per second is the basic measure unit — *B/s*).

This chart includes volume of transferred data in the selected direction in certain time intervals (depending on the selected period). The green curve represents volume of incoming data (download) in a selected time period, while the area below the curve represents the total volume of data transferred in the period. The red curve and area provide the same information for outgoing data (upload). Below the chart, basic statistic information, such as volume of data currently transferred (in the last interval) and the average and maximum data volume per an interval, is provided.

Select an option for *Picture size* to set a fixed format of the chart or to make it fit to the *Administration Console* screen.

17.2 Show connections related to the selected process

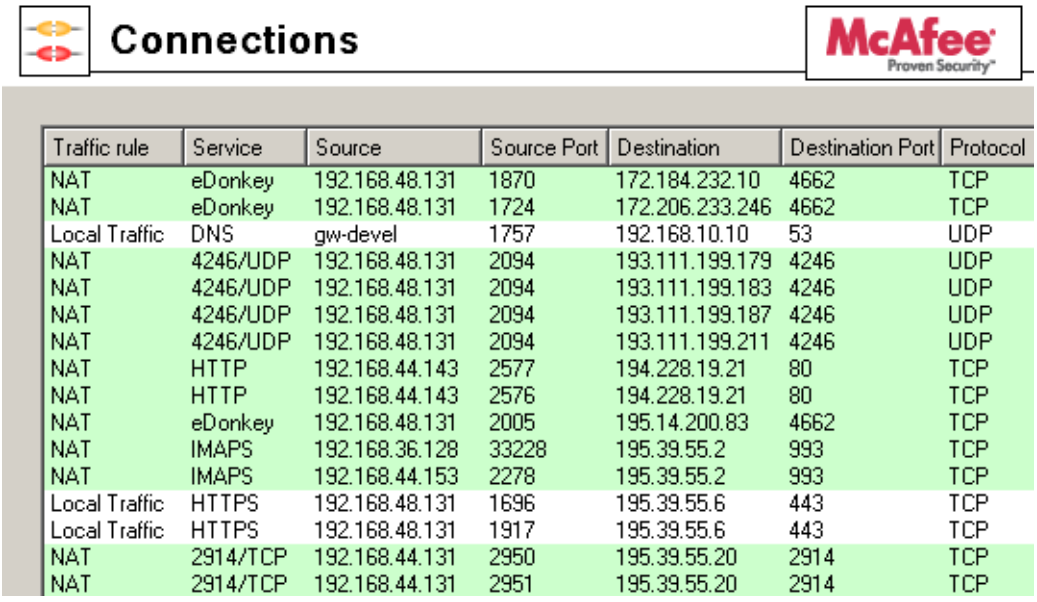
In *Status* → *Connections*, all the network connections which can be detected by *WinRoute* include the following:

- client connections to the Internet through *WinRoute*
- connections from the host on which *WinRoute* is running
- connections from other hosts to services provided by the host with *WinRoute*
- connections performed by clients within the Internet that are mapped to services running in LAN

WinRoute administrators are allowed to close any of the active connections.

Notes:

1. Connections among local clients will not be detected nor displayed by *WinRoute*.
2. UDP protocol is also called connectionless protocol. This protocol does not perform any connection. The communication is performed through individual messages (so-called datagrams). Periodic data exchange is monitored in this case.



Traffic rule	Service	Source	Source Port	Destination	Destination Port	Protocol
NAT	eDonkey	192.168.48.131	1870	172.184.232.10	4662	TCP
NAT	eDonkey	192.168.48.131	1724	172.206.233.246	4662	TCP
Local Traffic	DNS	gw-devel	1757	192.168.10.10	53	UDP
NAT	4246/UDP	192.168.48.131	2094	193.111.199.179	4246	UDP
NAT	4246/UDP	192.168.48.131	2094	193.111.199.183	4246	UDP
NAT	4246/UDP	192.168.48.131	2094	193.111.199.187	4246	UDP
NAT	4246/UDP	192.168.48.131	2094	193.111.199.211	4246	UDP
NAT	HTTP	192.168.44.143	2577	194.228.19.21	80	TCP
NAT	HTTP	192.168.44.143	2576	194.228.19.21	80	TCP
NAT	eDonkey	192.168.48.131	2005	195.14.200.83	4662	TCP
NAT	IMAPS	192.168.36.128	33228	195.39.55.2	993	TCP
NAT	IMAPS	192.168.44.153	2278	195.39.55.2	993	TCP
Local Traffic	HTTPS	192.168.48.131	1696	195.39.55.6	443	TCP
Local Traffic	HTTPS	192.168.48.131	1917	195.39.55.6	443	TCP
NAT	2914/TCP	192.168.44.131	2950	195.39.55.20	2914	TCP
NAT	2914/TCP	192.168.44.131	2951	195.39.55.20	2914	TCP

Figure 17.7 Overview of all connections established via WinRoute

One connection is represented by each line of the *Connections* window. These are network connections, not user connections (each client program can occupy more than one connection at a given moment).

The columns contain the following information:

Traffic rule
Name of the *WinRoute* traffic rule (see chapter 6) by which the connection was allowed.

Service
Name of transmitted service (if such service is defined in *WinRoute* — see chapter 12.3). If the service is not defined in *WinRoute*, the corresponding port number and protocol will be displayed instead (e.g. *5004/UDP*).

Source, Destination
IP address of the source (the connection initiator) and of the destination. If there is an appropriate reverse record in DNS, the IP address will be substituted with the DNS name.

The following columns are hidden by default. They can be enabled through the *Modify columns* dialog opened from the context menu (for details, see chapter 3.2).

Source port, Destination port
Ports used for the particular connection.

Protocol
Communication protocol (*TCP* or *UDP*)

Timeout
Time left until automatic disconnection. The countdown starts when data traffic stops. Each new data packet sets the counter to zero.

Rx, Tx
Total size of data received (*Rx*) or transmitted (*Tx*) during the connection (in kilobytes). Received data means the data transferred from *Source* to *Destination*, transmitted data means the opposite.

Info
An informational text describing the connection (e.g. about the protocol inspector applied to the connection).

Information in *Connections* is refreshed automatically within a user defined interval or the *Refresh* button can be used for manual refreshing.

Options of the Connections Dialog

The following options are available below the list of connections:

- *Hide local connections* — connections from or/and to the *WinRoute* host will not be displayed in the *Connections* window.

  This option only makes the list better-arranged and distinguishes connections of other hosts in the local network from the *WinRoute* host's connections.

- *Show DNS names* — this option displays DNS names instead of IP addresses. If a DNS name is not resolved for a certain connection, the IP address will be displayed.

Right-click on the *Connections* window (on the connection selected) to view a context menu including the following options:

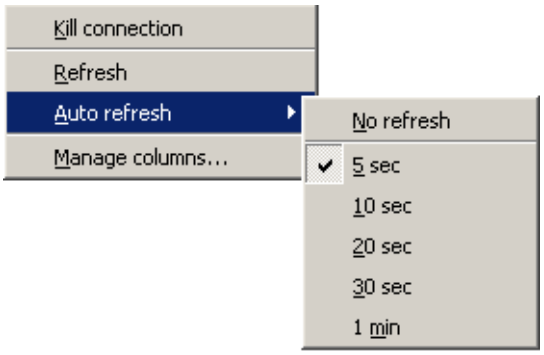


Figure 17.8 Context menu for Connections

Kill connection
: Use this option to finish selected connection immediately (in case of UDP connections all following datagrams will be dropped).
Note: This option is active only if the context menu has been called by right-clicking on a particular connection. If called up by right-clicking in the *Connections* window (with no connection selected), the option is inactive.

Refresh
: This option will refresh the information in the *Connections* window immediately. This function is equal to the function of the *Refresh* button at the bottom of the window.

Auto refresh
: Settings for automatic refreshing of the information in the *Connections* window. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Manage Columns

By choosing this option you can select which columns will be displayed in the *Connections* window (see chapter 3.2).

Color Settings

Clicking on the *Colors* button displays the color settings dialog to define colors for each connection:

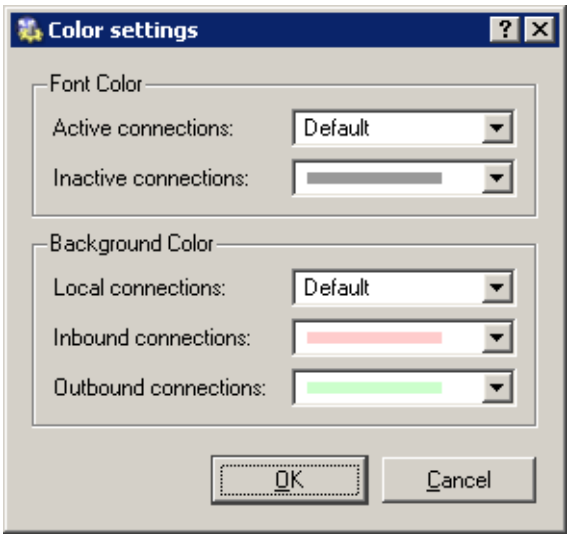


Figure 17.9 Connection colors settings

For each item either a color or the *Default* option can be chosen. Default colors are set in the operating system (the common setting for default colors is black font and white background).

Font Color

- *Active connections* — connections with currently active data traffic
- *Inactive connections* — TCP connections which have been closed but 2 minutes after they were killed they are still kept active — to avoid repeated packet mishandling)

Background Color

- *Local connections* — connections where an IP address of the host with *WinRoute* is either source or destination
- *Inbound connections* — connections from the Internet to the local network (allowed by firewall)
- *Outbound connections* — connections from the local network to the Internet

Note: Incoming and outgoing connections are distinguished by detection of direction of IP addresses — "out" (*SNAT*) or "in" (*DNAT*). For details, refer to chapter 6.

17.3 Alerts

WinRoute enables automatic sending of messages informing the administrator about important events. This makes *WinRoute* administration more comfortable, since it is not necessary to connect to the firewall via the *Administration Console* too frequently to view all status information and logs (however, this does not mean that it is not worthy to do this occasionally).

WinRoute generates alert messages upon detection of any specific event for which alerts are preset. All alert messages are recorded into the *Alert* log (see chapter 20.3). The *WinRoute* administrator can specify which alerts will be sent to whom, as well as a format of the alerts. Sent alerts can be viewed in *Status* → *Alerts*.

Note: SMTP relay must be set in *WinRoute* (see chapter 16.4), otherwise alerting will not work.

Alerts Settings

Alerts settings can be configured in the *Alerts settings* tab under *Configuration* → *Accounting*.

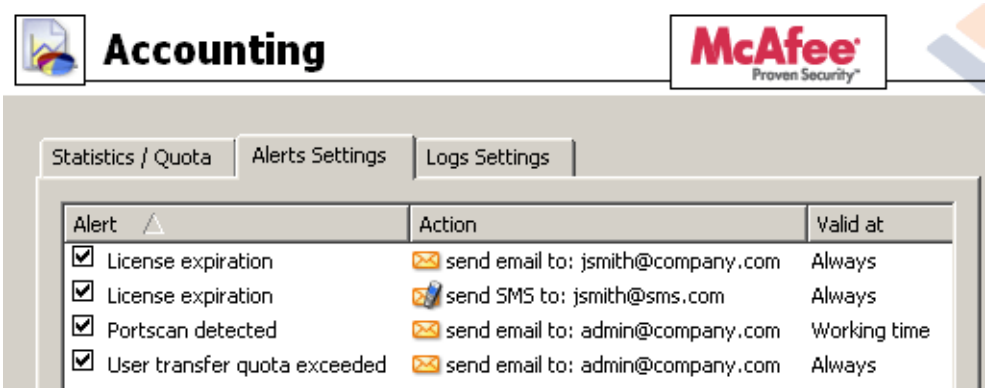


Figure 17.10 WinRoute Alerts

This tab provides list of "rules" for alert sending. Use checking boxes to enable/disable individual rules.

Use the *Add* or the *Edit* button to (re)define an alert rule.

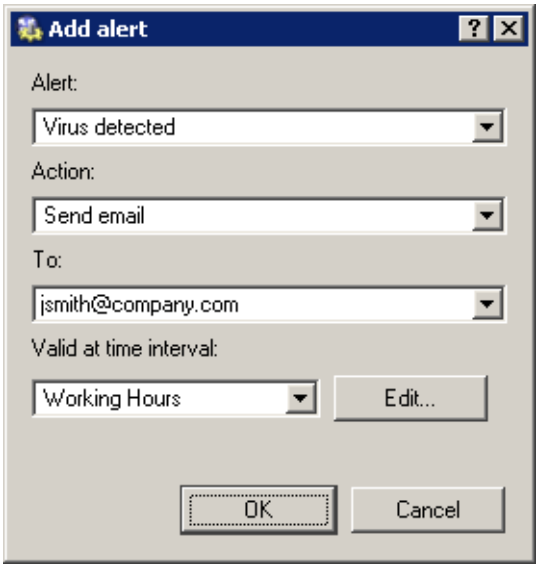


Figure 17.11 Alert Definitions

alert

Type of the event upon which the alert will be sent:

- *Virus detected* — antivirus engine has detected a virus in a file transmitted by HTTP, FTP, SMTP or POP3 (refer to chapter 11).
- *Portscan detected* — *WinRoute* has detected a *port scanning* attack (either an attack passing through or an attack addressed to the *WinRoute* host).
- *Host connection limit reached* — a host in the local network has reached the connection limit (see chapter 15.2). This may indicate deployment of an undesirable network application (e.g. Trojan horse or a spyware) on a corresponding host.
- *Low free disk space warning* — this alert warns the administrator that the free space of the *WinRoute* host is low (under 11 per cent of the total disk capacity). *WinRoute* needs enough disk space for saving of logs, statistics, configuration settings, temporary files (e.g. an installation archive of a new version or a file which is currently scanned by an antivirus engine) and other information. Whenever the *WinRoute* administrator receives such alert message, adequate actions should be performed immediately.
- *New version available* — a new version of *WinRoute* has been detected at the server of Kerio Technologies during an update check. The administrator can download this version from the server or from `http://www.kerio.com/` and install it using the *Administration Console* (see chapter 14.2).
- *User transfer quota exceeded* — a user has reached daily or monthly user transfer quota and *WinRoute* has responded by taking an appropriate action. For details, see chapter 13.1.
- *Connection failover event* — the Internet connection has failed and the system

was switched to a secondary line, or vice versa (it was switched back to the primary line). For details, refer to chapter 5.2.

- *License expiration* — expiration date for the corresponding *WinRoute* license/subscription (or license of any module integrated in *WinRoute*, such as *ISS OrangeWeb Filter*, the *McAfee* antivirus, etc.) is getting closer. The *WinRoute* administrator should check the expiration dates and prolong a corresponding license or subscription (for details, refer to chapter 4).
- *Dial / Hang-up of RAS line* *WinRoute* is dialing or hanging-up a RAS line (see chapter 5.1). The alert message provides detailed information on this event: line name, reason of the dialing, username and IP address of the host from which the request was sent.

Action

Method of how the user will be informed:

- *Send email* — information will be sent by an email message,
- *Send SMS (shortened email)* — short text message will be sent to the user's cell phone.
  Note: SMS messages are also sent as email. User of the corresponding cell phone must use an appropriate email address (e.g. `number@provider.com`). Sending of SMS to telephone numbers (for example via GSM gateways connected to the *WinRoute* host) is not supported.

To

Email address of the recipient or of his/her cell phone (related to the *Action* settings).
Recipients can be selected from the list of users (email addresses) used for other alerts or new email addresses can be added by hand.

Valid at time interval

Select a time interval in which the alert will be sent. Click *Edit* to edit the interval or to create a new one (details in chapter 12.2).

Alert Templates

Formats of alert messages (email or/and SMS) are defined by templates. Individual formats can be viewed in the *Status* → *Alerts* section of the *Administration Console*. Templates are predefined messages which include certain information (e.g. username, IP address, number of connections, virus information, etc.) defined through specific variables. *WinRoute* substitutes variables by corresponding values automatically. The *WinRoute* administrator can customize these templates.

Templates are stored in the `templates` subdirectory of the installation directory of *WinRoute*

`C:\Program Files\Kerio\WinRoute Firewall\templates` by default):

- the `console` subdirectory — messages displayed in the top section of *Status* → *Alerts* (overview),
- the `console\details` subdirectory — messages displayed at the bottom section of *Status* → *Alerts* (details),
- the `email` subdirectory — messages sent by email (each template contains a message in the plain text and HTML formats),
- the `sms` subdirectory — SMS messages sent to a cell phone.

Note: In the latest version of *WinRoute*, only English alerts are available (templates for other languages under `email` and `sms` subdirectories are ready for future versions).

Alerts overview (in Administration Console)

Overview of all sent alerts (defined in *Configuration* → *Accounting*) can be found under *Status* → *Alert Messages*. The language set in the *Administration Console* is used (if a template in a corresponding language is not found, the alert is displayed in English).

Overview of all sent alerts (sorted by dates and times) is provided in the top section of this window.

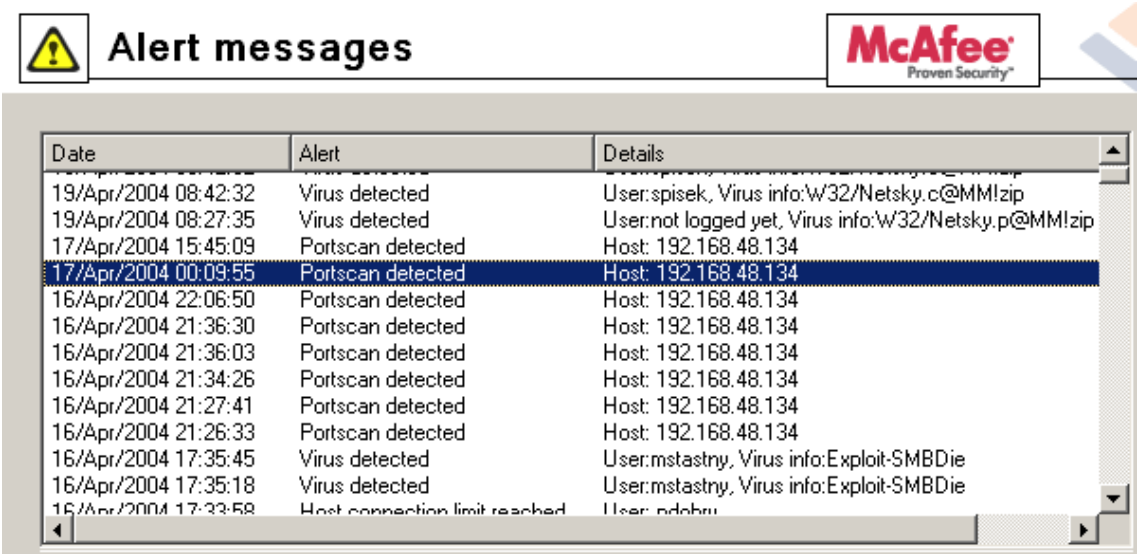

Alert messages
McAfee
Proven Security
Date
Alert
Details
19/Apr/2004 08:42:32 Virus detected User:spisek, Virus info:W32/Netsky.c@MM!zip
19/Apr/2004 08:27:35 Virus detected User:not logged yet, Virus info:W32/Netsky.p@MM!zip
17/Apr/2004 15:45:09 Portscan detected Host: 192.168.48.134
17/Apr/2004 00:09:55 Portscan detected Host: 192.168.48.134
16/Apr/2004 22:06:50 Portscan detected Host: 192.168.48.134
16/Apr/2004 21:36:30 Portscan detected Host: 192.168.48.134
16/Apr/2004 21:36:03 Portscan detected Host: 192.168.48.134
16/Apr/2004 21:34:26 Portscan detected Host: 192.168.48.134
16/Apr/2004 21:27:41 Portscan detected Host: 192.168.48.134
16/Apr/2004 21:26:33 Portscan detected Host: 192.168.48.134
16/Apr/2004 17:35:45 Virus detected User:mstastny, Virus info:Exploit-SMBDie
16/Apr/2004 17:35:18 Virus detected User:mstastny, Virus info:Exploit-SMBDie

Figure 17.12 Overview of sent alerts

Each line provides information on one alert:

- *Date* — date and time of the event,
- *Alert* — event type,
- *Details* — basic information on events (IP address, username, virus name, etc.).

Click an event to view detailed information on the item including a text description (defined by templates under `console\details` — see above) in the bottom section of the window.

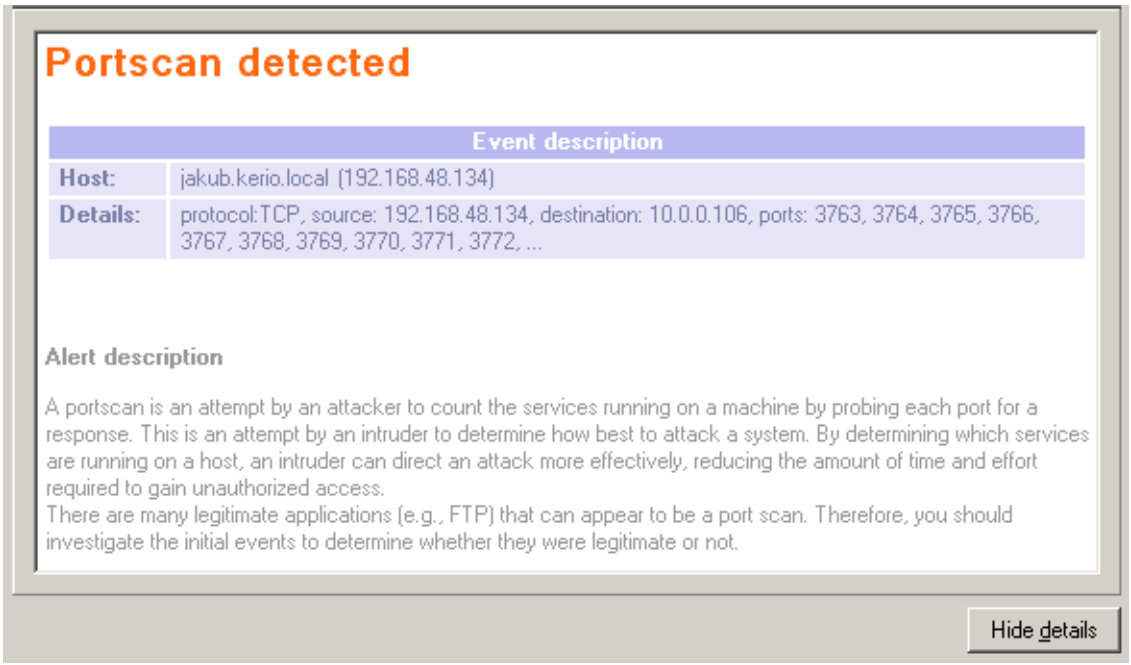

Portscan detected
Event description
Host:
jakub.kerio.local (192.168.48.134)
Details:
protocol:TCP, source: 192.168.48.134, destination: 10.0.0.106, ports: 3763, 3764, 3765, 3766, 3767, 3768, 3769, 3770, 3771, 3772, ...
Alert description
A portscan is an attempt by an attacker to count the services running on a machine by probing each port for a response. This is an attempt by an intruder to determine how best to attack a system. By determining which services are running on a host, an intruder can direct an attack more effectively, reducing the amount of time and effort required to gain unauthorized access.
There are many legitimate applications (e.g., FTP) that can appear to be a port scan. Therefore, you should investigate the initial events to determine whether they were legitimate or not.
Hide details

Figure 17.13 Details of a selected event

Note: Details can be optionally hidden or showed by clicking the *Hide/Show details* button (details are displayed by default).

Chapter 18

Basic statistics

Statistical information about users (volume of transmitted data, used services, categorization of web pages) as well as of network interfaces of the *WinRoute* host (volume of transmitted data, load on individual lines) can be viewed in *WinRoute*.

In the *Administration Console*, it is possible to view basic user statistics (volume of transferred data and quota usage information) and statistics of network interfaces (transferred data, traffic charts). Detailed statistics of users, web pages and volume of transferred data are available in the firewall's web interface (*Kerio StaR* — see chapter 19).

18.1 Interface statistics

The *Interface statistics* tab in *Status* → *Statistics* provides detailed information on volume of data transmitted in both directions through individual interfaces of the *WinRoute* host in selected time intervals (today, this week, this month, total).

Interfaces can be represented by network adapters, dial-ups or VPN tunnels. *VPN server* is a special interface — communication of all VPN clients is represented by this item in *Interface statistics*.

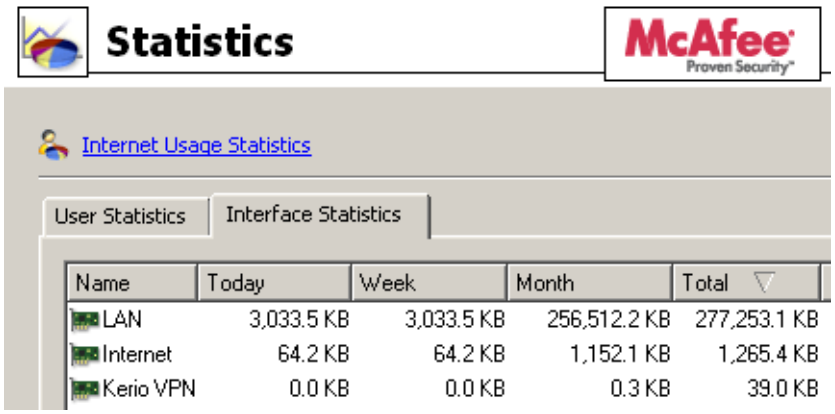


Figure 18.1 Firewall's interface statistics

Optionally, other columns providing information on volume of data transmitted in individual time periods in both directions can be displayed. Direction of data transmission is related to the interface (the *IN* direction stands for data received by the interface, while *OUT* represents data sent from the interface).

Example: The *WinRoute* host connects to the Internet through the *Public* interface and the local network is connected to the *LAN* interface. A local user downloads 10 MB of data from the Internet. This data will be counted as follows:

- *IN* at the *Public* interface is counted as an *IN* item (data from the Internet was received through this interface),
- at the *LAN* interface as *OUT* (data was sent to the local network through this interface).

Note: Interface statistics are saved into the `stats.cfg` configuration file in the *WinRoute's* installation directory. This implies that they are not reset when the *WinRoute Firewall Engine* is closed.

Interface Statistics menu

A context menu providing the following options will be opened upon right-clicking anywhere in the table (or on a specific interface):

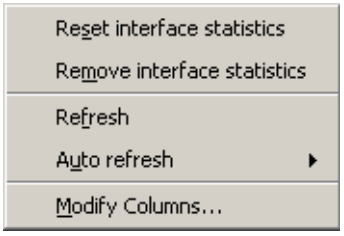


Figure 18.2 Context menu for Interface statistics

Reset interface statistics
: This option resets statistics of the selected interface. It is available only if the mouse pointer is hovering an interface at the moment when the context menu is opened.

Refresh
: This option will refresh the information on the *Interface Statistics* tab immediately. This function is equal to the function of the *Refresh* button at the bottom of the window.

Auto refresh

Settings for automatic refreshing of the information on the *Interface Statistics* tab. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Manage Columns

Use this option to select and unselect items (columns) which will (not) be displayed in the table (see chapter 3.2).

Remove interface statistics

This option removes the selected interface from the statistics. Only inactive interfaces (i.e. disconnected network adapters, hung-up dial-ups, disconnected VPN tunnels or VPN servers which no client is currently connected to) can be removed. Whenever a removed interface is activated again (upon connection of the VPN tunnel, etc.), it is added to the statistics automatically.

Graphical view of interface load

The traffic processes for a selected interface (transfer speed in *B/s*) and a specific time period can be viewed in the chart provided in the bottom window of the *Interface statistics* tab. Use the *Show details / Hide details* button to show or hide this chart (the show mode is set by default).

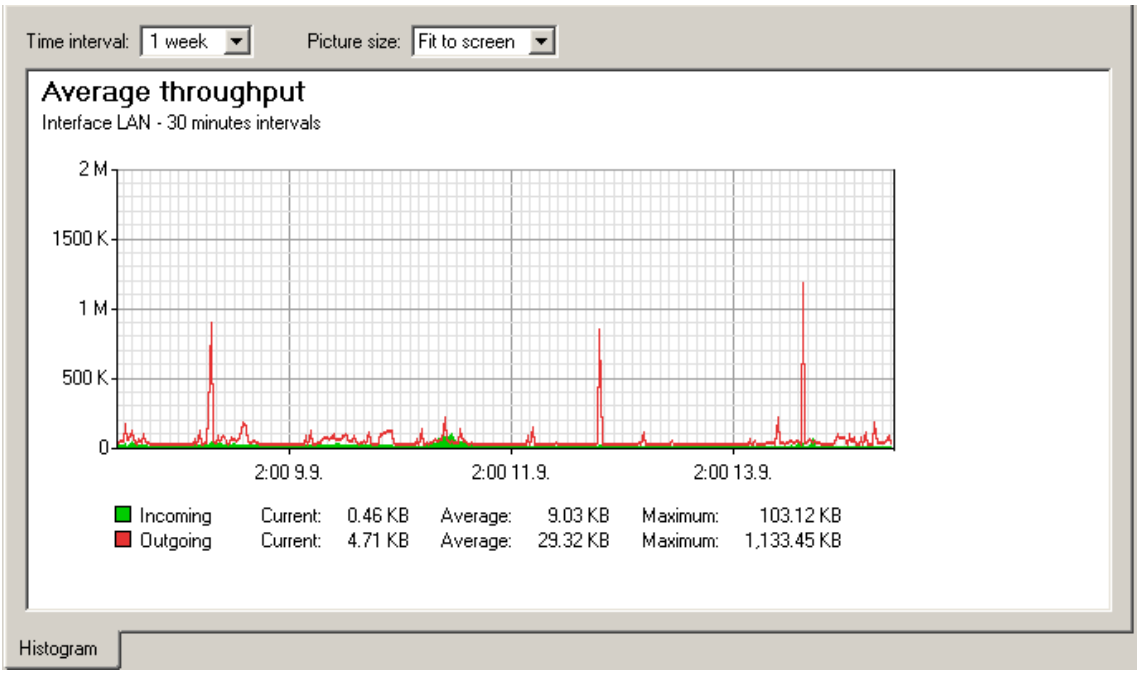


Figure 18.3 Chart informing about average throughput at the interface

The period (*2 hours* or *1 day*) can be selected in the *Time interval* box. The selected time range is always understood as the time until now ("last 2 hours" or "last 24 hours").

The x axis of the chart represents time and the y axis represents traffic speed. The x axis is measured accordingly to a selected time period, while measurement of the y axis depends on the maximal value of the time interval and is set automatically (bytes per second is the basic measure unit — *B/s*).

The legend above the graph shows the sampling interval (i.e. the time for which a sum of connections or messages is counted and is displayed in the graph).

Example: Suppose the *1 day* interval is selected. Then, an impulse unit is represented by 5 minutes. This means that every 5 minutes an average traffic speed for the last 5 minutes is recorded in the chart.

Select an option for *Picture size* to set a fixed format of the chart or to make it fit to the *Administration Console* screen.

18.2 User Statistics — data volumes and quotas

The *User Statistics* of the *Status* → *Statistics* section provides detailed statistics on volume of data transmitted by individual users during various time periods (today, this week, this month and total).

The *Quota* column provides usage of transfer quota by a particular user in percents (see chapter 13.1). Colors are used for better reference:

- green — 0%–74% of the quota is used
- yellow — 75%–99% of the quota is used
- red — 100% (limit reached)

Notes:

1. User quota consists of two limits: daily and monthly. The *Quota* column provides the higher value of the two percentual values (if the daily usage is 50% of the daily quota and the monthly usage is 75%, the yellowed *75%* value is displayed in the *Quota* column).
2. Monthly quota is reset automatically at the beginning of an accounting period. This period may differ from a civil month (see chapter 19.2).

The *all users* line provides total volume of data transmitted by all users in the table (even of the unrecognized ones). The *unrecognized users* item includes all users who are currently not authenticated at the firewall. These lines do not include quota usage information.

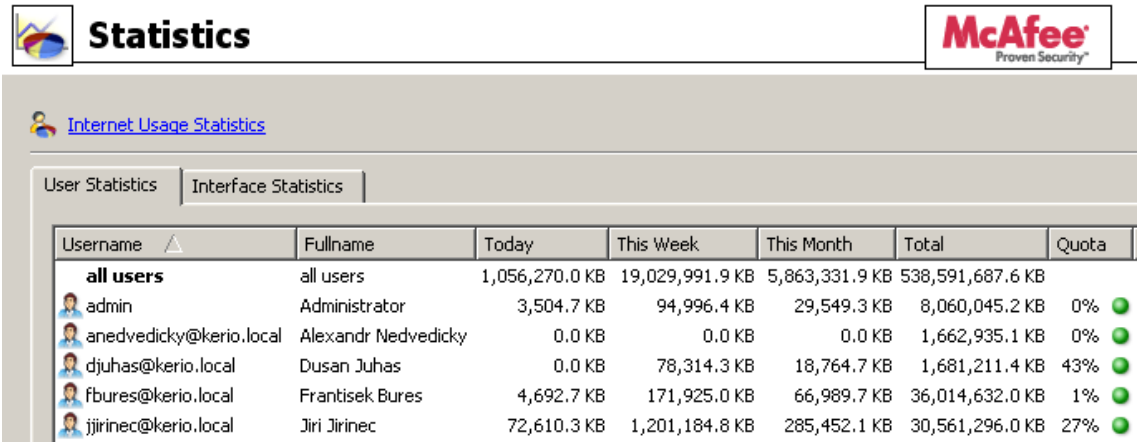


Figure 18.4 User statistics

Notes:

1. Optionally, other columns providing information on volume of data transmitted in individual time periods in both directions can be displayed. Direction of data transmission is related to the user (the *IN* direction stands for data received by the user, while *OUT* represents data sent by the user).

2. User statistics are saved in the `stats.cfg` file under the *WinRoute* directory. This implies that this data will be saved the next time the *WinRoute Firewall Engine* will be started.

User Statistics dialog options

Right-click on the table (or on an item of a selected user) to open the context menu with the following options:

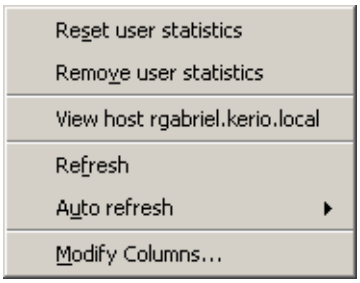


Figure 18.5 Context menu for User statistics

Reset user statistics

This option resets statistics of the selected user.

Warning: Be aware that using this option for the *all users* item resets statistics of all users, including unrecognized ones!

Note: Values in the statistics are also used for user traffic quota purposes (see chapter 13.1). Reset of user statistics also unblocks traffic of the particular user in case that the traffic has been blocked for quota reasons.

Remove user statistics

Removes the item including the user's statistics. This option is helpful for reference purposes only (e.g. to exclude blocked user accounts from the list, etc.). Removed accounts will be added to the statistics automatically when data in the particular account is changed (e.g. when we unblocked an account and its user connects and starts to communicate again).

Total statistics including all users and statistics of unrecognized users cannot be removed.

Note: Corresponding statistics are reset automatically when a user is removed from the list.

View host...

This option is not available unless the selected user is connected to the firewall. The *View host* option switches to the *Status* → *Active Hosts* section of the host the particular user is connected from.

Refresh

This option will refresh the information on the *User Statistics* tab immediately. This function is equal to the function of the *Refresh* button at the bottom of the window.

Auto refresh

Settings for automatic refreshing of the information on the *User Statistics* tab. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Manage Columns

Use this option to select and unselect items (columns) which will (not) be displayed in the table (see chapter 3.2).

Chapter 19

Kerio StaR — statistics and reporting

The *WinRoute's* web interface provides detailed statistics on users, volume of transferred data, visited websites and web categories. This information may help figure out browsing activities and habits of individual users.

The statistics monitor the traffic between the local network and the Internet. Volumes of data transferred between local hosts and visited web pages located on local servers are not included in the statistics (also for technical reasons).

One of the benefits of web statistics and reports is their high availability. The user (usually an office manager) does not need the *Administration Console* and they even do not need *WinRoute* administrator rights (special rights are used for statistics). Statistics viewed in web browsers can also be easily printed or saved on the dick as web pages.

Notes:

1. The *WinRoute* administrator should inform users that their browsing activities are monitored by the firewall.
2. Statistics and reports in *WinRoute* should be used for reference only. It is highly unrecommended to use them for example to figure out exact numbers of Internet connection costs per user.

19.1 Monitoring and storage of statistic data

Diverse data is needed to be gathered for the statistics. Statistic data is stored in the database (the `star` subdirectory of the *WinRoute's* installation directory — for details, see chapter 23.2). Total period length for which *WinRoute* keeps the statistics can be set in the *Accounting* section of the *Administration Console* (see chapter 19.2). By default, this time is set to *24 months* (i.e. 2 years).

For technical reasons, the *WinRoute Firewall Engine* stores gathered statistic data in the cache (the `star\cache` subdirectory) and data is recorded in the database once per hour. The cache is represented by several files on the disk. This implies that any data is kept in the cache even if the *WinRoute Firewall Engine* is stopped or another problem occurs (failure of power supply, etc.) though not having been stored in the database yet.

The statistics use data from the main database. This implies that current traffic of individual users is not included in the statistics immediately but when the started period expires and the data is written in the database.

Note: Data in the database used for statistics cannot be removed manually (such action would be meaningless). In statistics, it is possible to switch into another view mode where data is related only to a period we need to be informed about. If you do not wish to keep older data, it is possible to change the statistics storage period (see above).

Requirements of the statistics

The following conditions must be met for correct function of all statistics:

- The firewall should always require user authentication. The statistics by individual users would not match the true state if unauthenticated users are allowed to access the Internet. For details see chapter 8.

- For statistics on visited websites, it is necessary that a corresponding protocol inspector is applied to any *HTTP* traffic. This condition is met by default unless special traffic rules disabling the particular protocol inspector are applied (see chapter 23.4).

  If the *WinRoute* proxy server is used, visited pages are monitored by the proxy server itself (see chapter 5.5).

  Note: HTTPS traffic is encrypted and, therefore, it is impossible to monitor visited sites and categories. Only volume of transferred data is included in the statistics for such traffic.

- For monitoring of web categories of visited websites, the *ISS OrangeWeb Filter* module must be enabled.. In its configuration, the *Categorize each page regardless of HTTP rules* option should be enabled, otherwise web categories statistics would be unreliable. For details, see chapter 10.4.

19.2 Settings for statistics and quota

Under certain circumstances (too many connected users, great volume of transmitted data, low capacity of the *WinRoute* host, etc.), viewing of statistics may slow *WinRoute* and data transmission (Internet connection) down. Be aware of this fact while opening the statistics. Therefore, *WinRoute* allows such configuration of statistics that is customized so that only useful data is gathered and useful statistics created. If you do not wish to use statistics, it is possible to disable them (this will increase processor's performance and save disk space of the *WinRoute* host).

Statistics and their parameters can be set in the *Statistics / Quota* tab under *Configuration → Accounting*.

Note: These settings do not affect basic user and interface statistics available in the *Administration Console* (see chapter 18).

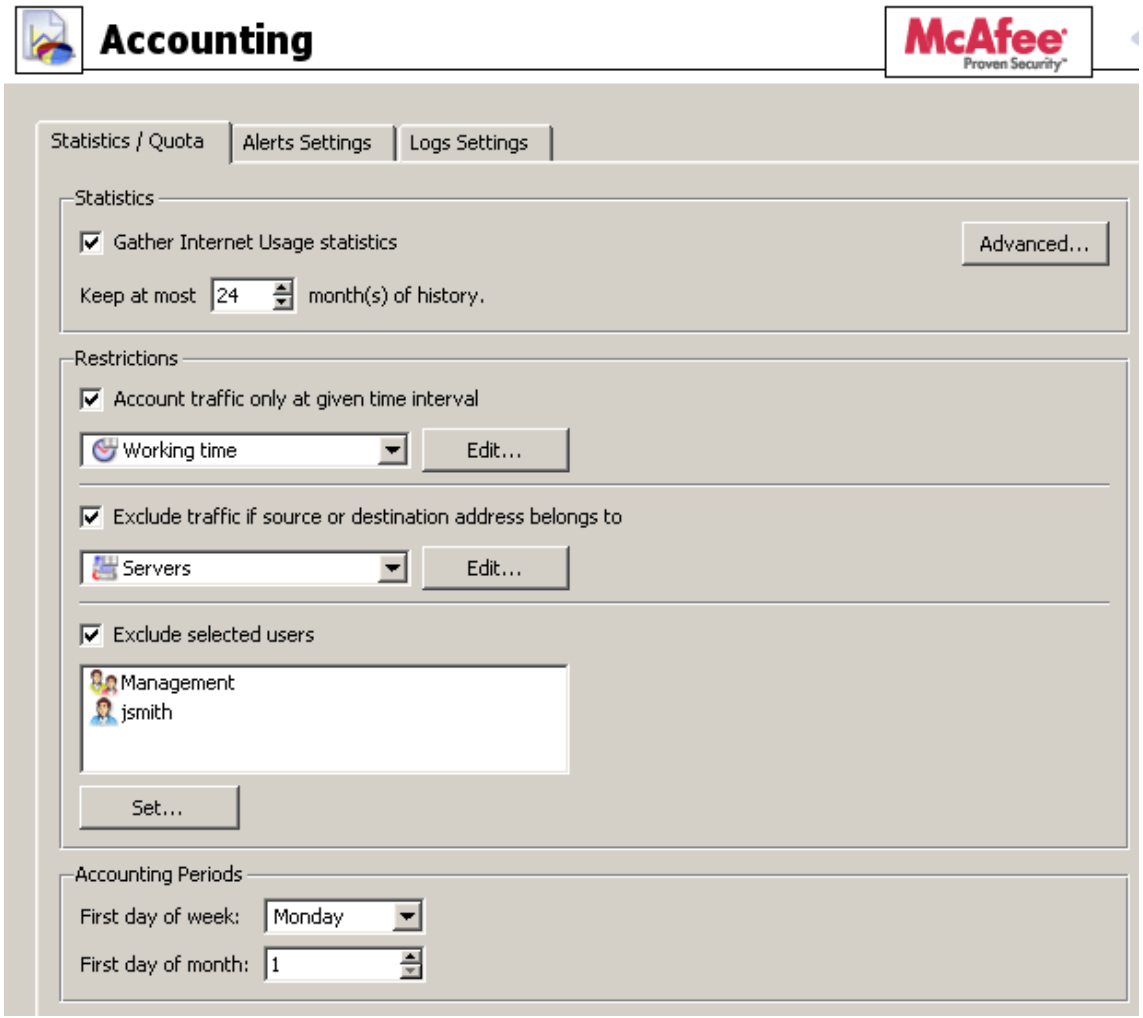


Figure 19.1 Statistics and transferred data quota settings

Enable/disable gathering of statistic data

The *Gather Internet Usage statistics* option enables/disables all statistics (i.e. stops gathering of data for statistics).

You can use the *Keep at most...* option to specify a time period for which the data will be kept (i.e. the age of the oldest data that will be available). This option affects disk space needed for the statistics remarkably. To save disk space, it is therefore recommended to keep the statistics only for a necessary period.

Advanced settings for statistics

The *Advanced* button opens a dialog where parameters can be set for viewing of statistics in the *Kerio StaR* interface (see chapter 18).

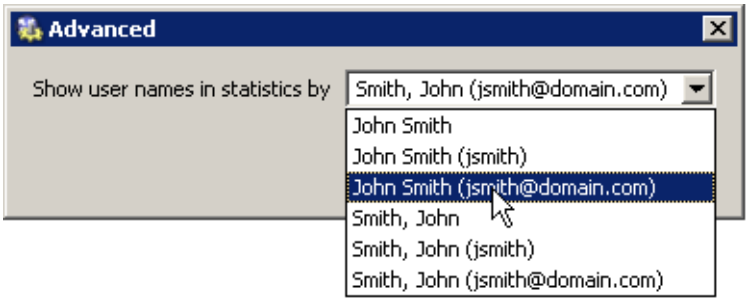


Figure 19.2 Kerio StaR advanced options

The *Show user names in statistics by...* option enables select a mode of how users and their names will be displayed in individual user statistics. Full names can be displayed as *first name second name* or *second name, first name*. Optionally, it is also possible to view full names followed by username without or with domain (if *Active Directory* mapping is used).

Statistics and quota restrictions

In the *Restrictions* section, it is possible to define restrictions for statistics and for transferred data quota.

The purpose of the restrictions is to gather only useful information to keep the statistics simple and clear and also to eliminate useless data (this saves disk space). Usage of individual restrictions:

- *Time interval* — define a time period when information will be included in statistics and quota (e.g. only in working hours). Without this period, no traffic will be included in the statistics and in the quota neither.
  For details on time intervals, see chapter 12.2.
- *IP addresses* — define IP addresses of hosts which will be excluded from the statistics and to which quota will not be applied.
  The selected group may include both local or Internet IP addresses. If any of these IP addresses belongs to the local network, bear in mind that no traffic of the host will be included in the statistics or the quota. In case of addresses of Internet servers, traffic of local users with the server will not be accounted in the statistics or any user quota.
  For details on IP groups, see chapter 12.1.
- *Exclude selected users* — select users and/or user groups which will be excluded from the statistics and no quota will be applied to them. This setting has the highest priority and overrules any other quota settings in user or group preferences.
  For details on users and groups, see chapter 13.

Statistics and quota accounting periods

Accounting period is a time period within which information of transferred data volume and other information is gathered. Statistics enable generating of weekly and monthly overviews. In *Accounting Periods*, it is possible to define starting days for weekly and monthly periods (for example, in statistics, a month can start on day 15 of the civil month and end on day 14 of the following civil month). For details, see chapter 19.4.

The parameter of first day of monthly period also sets when the monthly transferred data counter of individual users will be set to zero (for monthly quota details, see chapter 13.1 and 9.3).

19.3 Connection to StaR and viewing statistics

To view statistics, user must authenticate at the *WinRoute's* web interface first. User (or the group the user belongs to) needs rights for statistics viewing — see chapter 13.1. *StaR* can be accessed by several methods, depending on whether connecting from the *WinRoute* host (locally) or from another host (remotely).

Note: For details on the *WinRoute's* web interface, see chapter 9.2.

Accessing the statistics from the WinRoute host

On the *WinRoute* host, the *StaR* may be opened as follows:

- By using the *Internet Usage Statistics* link available in the *WinRoute Engine Monitor* context menu (opened by the corresponding icon in the notification area — see chapter 2.5).
- By using the *Internet Usage Statistics* link under *Start* → *Programs* → *Kerio* → *WinRoute Firewall*.

Both links open the unsecured *StaR* interface directly on the local host (by default `http://localhost:4080/star`) using the default web browser.

Note: Within local systems, secured traffic would be useless and the browser would bother user with needless alerts.

Remote access to the statistics

It is also possible to access the statistics remotely, i.e. from any host which is allowed to connect to the *WinRoute* host and the web interface's ports, by using the following methods:

- If the host is connected to *WinRoute* by the *Administration Console*, the *Internet Usage Statistics* link available under *Status* → *Statistics* can be used. This link opens the secured *StaR* interface for statistics in the default web browser.

Note: URL for this link consists of the name of the server and of the port of the secured Web interface defined in the configuration (see chapter 9.1). This guarantees function of the link from the *WinRoute* host and from the local network. To make *Internate Usage Statistics* link work also for remote administration over the Internet, name of the particular server must be defined in the public DNS (with the IP address of the particular firewall) and traffic rules must allow access to the port of the secured Web interface(4081 by default).

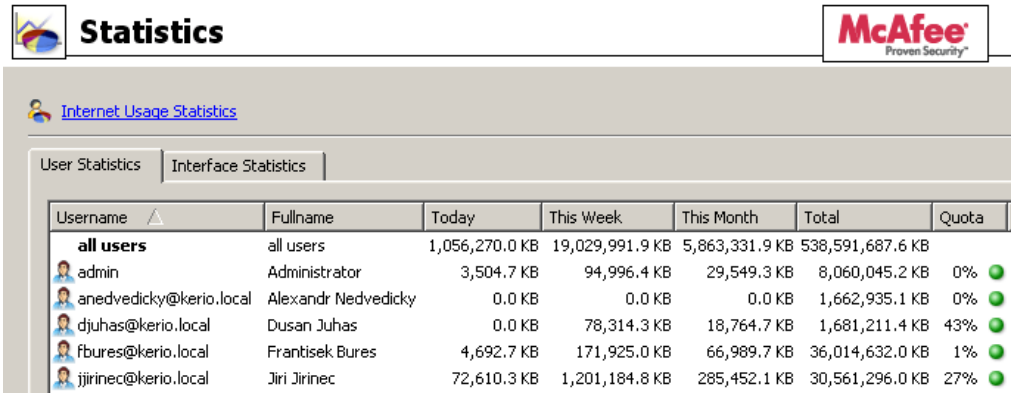


Figure 19.3 Link for viewing of the statistics in the Administration Console (status → Statistics)

- At `https://server:4081/star` or `http://server:4080/star` This URL works for the *StaR* only. If the user has not appropriate rights to view statistics, an error is reported.
- At `https://server:4081/` or `http://server:4080/`. This is the primary URL of the *WinRoute's* web interface. If the user possesses appropriate rights for stats viewing, the *StaR* welcome page providing overall statistics (see below) is displayed. Otherwise, the *My Account* page is opened (this page is available to any user).

Warning: In case of access via the Internet (i.e. from a remote host) it is recommended to use only the secured version of the web interface. The other option would be too risky.

StaR page in the web interface

The page is divided into the following tabs:

- *Overall* — overall statistics including traffic of all local users (volumes of transferred data, top users, top web pages, etc.). This section is opened as a welcome page immediately upon a successful logon.
- *Individual* — statistics of individual users (volumes of transferred data, top web pages visited by the user, etc.).

- *Users by Traffic* — table and chart for volumes of data transferred by individual users.
- *Visited Sites* — overview of the ten most frequently visited web domains. A chart and table of top users having visited the greatest number of web pages of the domain is provided.
- *Web Categories* — the top ten most frequently visited web categories (in accordance with the *ISS OrangeWeb Filter's* categorization). A chart referring to each web category is provided, along with table of users with the highest number of requests for sites belonging to the particular category..

Detailed descriptions of individual sections are provided in the following chapters.

19.4 Accounting period

Most frequently, statistic information needed refer to a certain time period (today, last week, etc.). This period is called *accounting period*.

The *Change Period* option at the top of the page can be used to set this parameter.

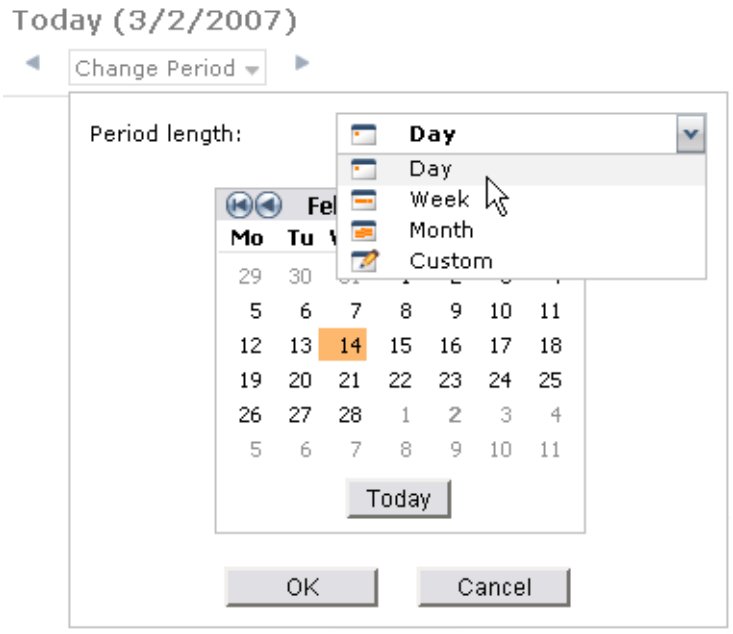


Figure 19.4 Selection of accounting period

Select an item in the *Period length* combo box (day, week, month). Further options are displayed depending on which option has been selected.

Note: Weeks and months might not correspond with weeks and months of the civil calendar. In configuration of statistics (see chapter 19.2), it is possible to set so called accounting period — starting day of a month and the first day in a week. Changes in these settings affect only new data. The data already having been stored in the database stay the same as before the change.

It is also possible to set a custom accounting period, defined by starting and ending days.

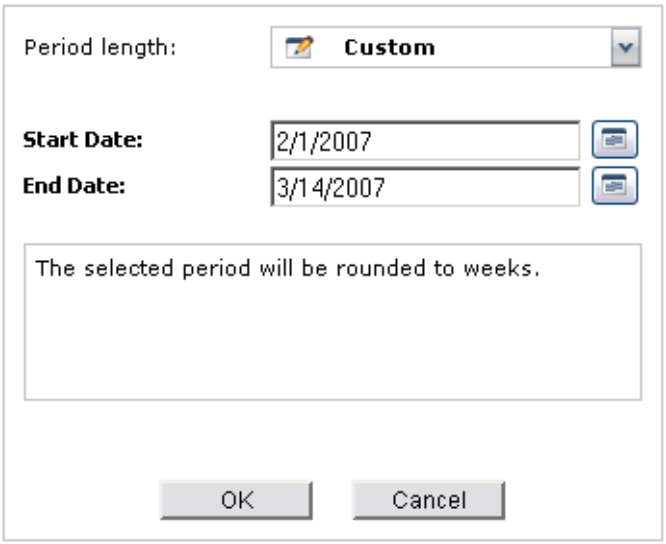


Figure 19.5 Custom accounting period

The starting and ending day can be defined manually or selected from the thumbnail calendar available upon clicking on the icon next to the corresponding textfield.

Note: Under certain circumstances, an information may be reported that this period will be rounded to whole weeks or months. The limits are applied for technical reasons (such as the chart limits, etc.). In such a case, the real (rounded) period for the statistics will be shown above the *Change Period* button.

The left and right arrows at the *Change Period* button can be used to browse the previous or following periods of the selected length. This browsing is not available for custom accounting periods.

The selected period applies to all tabs until a next selection (or until closing of the *Kerio StaR* interface). The “today” period is set as default and used upon each startup of the *Kerio StaR* interface.

19.5 Overall View

The *Overall* tab provides overall statistics for all users within the local network (including anonymous, i.e. unauthenticated users) for the selected accounting period.

Traffic by periods

The first chart provides information on the volume of data transferred in individual subperiods of the selected period. The table next to the chart informs on data volumes transferred in the entire selected period (total and for both directions as well). Simply hover a column in the chart with the mouse pointer to view volume of data transferred in the corresponding subperiod. Click on a column in the chart to switch to the information on the particular subperiod only[6] (for details, see chapter 19.4.

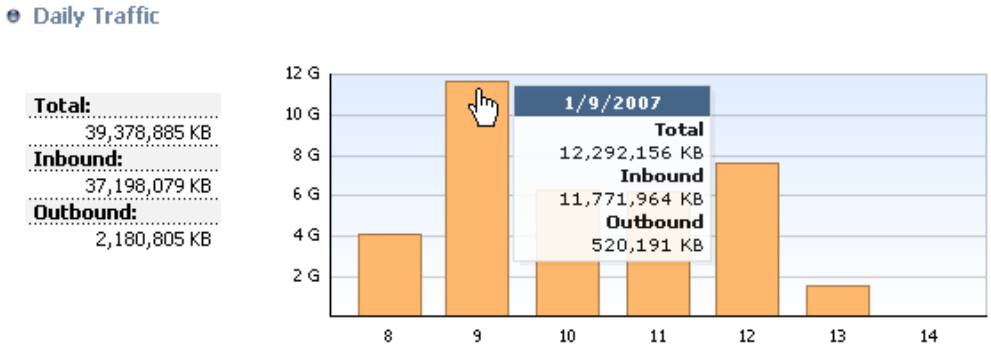


Figure 19.6 Daily Traffic

The subperiod length depends on the current period:

- *day* — the chart shows traffic by hours,
- *week* or *month*— the chart shows traffic by days.

For custom periods:

- *up to 2 days* — the chart shows traffic by hours,
- *up to 5 weeks* — the chart shows traffic by days,
- *up to 6 months* — the chart shows traffic by weeks,
- *more than 6 months* — the chart shows traffic by months,

Top Visited Websites

The chart of the most frequented websites shows top five domains by their visit rate. The number in the chart refers to number of visits of all web pages of the particular domain in the selected accounting period.

Note: The *HTTP* protocol inspector "sees" only individual HTTP requests. To count number of visited pages (i.e. to recognize which requests were sent within a single visit), *WinRoute* uses a special heuristic algorithm. The information, therefore,

[6] It is not possible to switch to a selected subperiod if the traffic is displayed by hours. The shortest accounting period to be selected is one day.

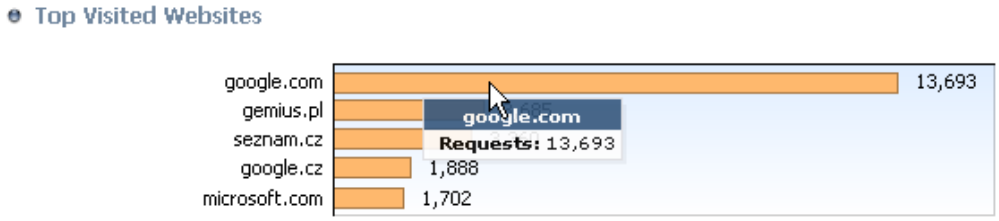


Figure 19.7 Chart of top visited web domains

cannot be precise, though the approximation is very good.

Top Requested Web Categories

This chart shows top five web categories requested in the selected period sorted by the *ISS OrangeWeb Filter* module. The number in the chart refers to total number of HTTP requests included in the particular category. For technical reasons, it is not possible to recognize whether the number includes requests to a single page or to multiple pages. Therefore, number of requests is usually much higher than number of visited websites in the previous chart.

For details on web categories, refer to chapter 10.4.

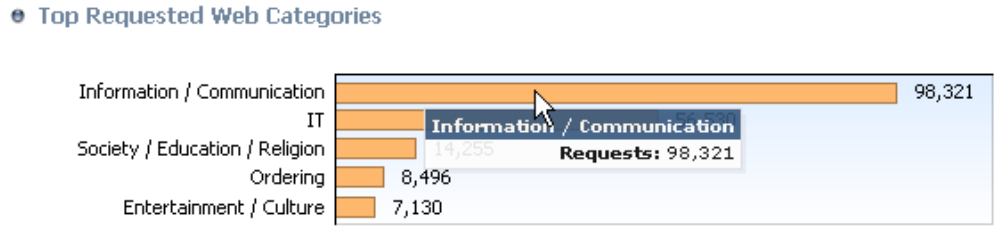


Figure 19.8 The chart of top requested web categories

Top 5 users

Top five users, i.e. users with the greatest volume of data transferred in the selected accounting period.

The chart includes individual users and total volume of transferred data.

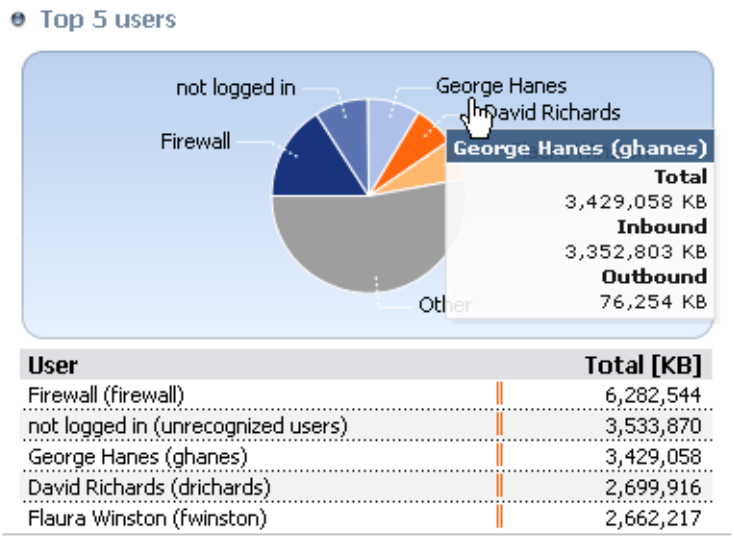
The chart shows part of the most active users in the total volume of transferred data in the selected period. Hover a user's name in the chart by the mouse pointer to see volume of data transferred by the user, both in total numbers and both directions (download, upload).

Click on a user's name in the chart or in the table to switch to the *Individual* tab (see chapter 19.6) where statistics for the particular user are shown.

These charts and tables provide useful information on which users use the Internet connection the most and make it possible to set necessary limits and quotas.

Notes:

1. Total volume of data transferred by a particular user is a summary of data transferred by the user from all hosts from which they have connected to the firewall in the selected period.



User	Total [KB]
Firewall (firewall)	6,282,544
not logged in (unrecognized users)	3,533,870
George Hanes (ghanes)	3,429,058
David Richards (drichards)	2,699,916
Flaura Winston (fwinston)	2,662,217

Figure 19.9 Top 5 users statistics

2. *Firewall* is a special user account including data transferred from and to the *WinRoute* host. However, whenever a particular user connects to the firewall, the data transferred are accounted in statistics of this user.
3. Data transferred by unauthenticated users is summed and accounted as the *not logged in* user. However, this information is not very useful and, therefore, it is recommended to set firewall to always require authentication. For details, see chapter 8.1.

TIP: The way of users' names are displayed in the table can be set in the *Administration Console*, in section *Accounting*, after clicking on the *Advanced* button (see chapter 19.2). Only full names are shown in charts (or usernames if the full name is not defined in the account of the particular user).

Used Protocol

The chart of used protocols shows part of individual protocols (i.e. their classes) in the total volume of data transferred in the selected accounting period. Hover a protocol name with the mouse pointer to see volume of data transferred by the particular protocol.

Such information might, for example, help recognize type of traffic between the local network and the Internet. If the internet line is overloaded, it is possible to use the information to set necessary limits and restrictions (traffic rules, URL rules, etc.).

For better reference, *WinRoute* sorts protocols to predefined classes:

- *Web* — *HTTP* and *HTTPS* protocols and any other traffic served by the *HTTP* protocol inspector (see chapter 6.3),
- *Proxy* — connections to the Internet via the *WinRoute* proxy server,

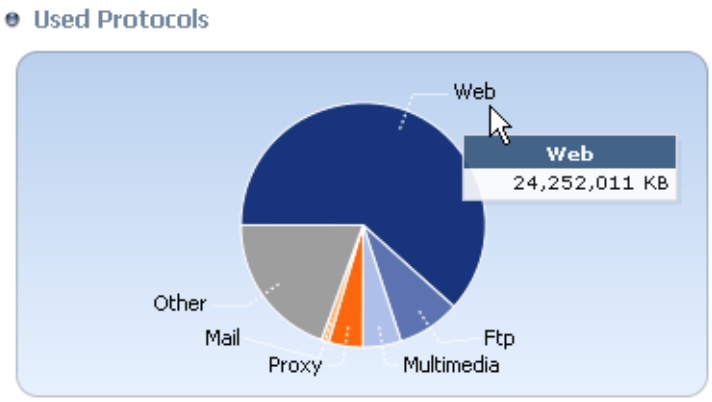


Figure 19.10 Parts of individual protocols in the total volume of transferred data

- *E-mail* — *SMTP*, *IMAP*, *POP3* protocols (and their secured versions),
- *FTP* — *FTP* protocol (including traffic over proxy server),
- *Multimedia* — protocols enabling real-time transmission of sound and video files (e.g. *RTSP*, *MMS*, *RealAudio*),
- *P2P* — file-sharing protocols (*peer-to-peer* — e.g. *DirectConnect*, *BitTorrent*, *eDonkey*, etc.). The traffic is accounted only if *WinRoute* detects that it is traffic within a *P2P* network. This issue is described in chapter 15.1.
- *Other* — any traffic which does not belong to any of the previously described categories.

Notes:

1. The *No data available* alert informs that no data is available in *WinRoute's* database for the selected statistics and accounting period. This issue may be caused by various reasons — for example, any of the conditions described in chapter 19.1 is not met, the selected user account did or does not exist in the selected period, the user has not connected to the firewall in the period, etc.

2. *WinRoute* tries to optimize size of the statistic database and volume of processed data. The greatest volume of data is generated by statistics of visited websites. For this reason, daily statistics of visited websites are kept only for the last 40 days. Weekly and monthly statistics are available for the entire data storage period as set in the configuration (see chapter 19.2).

   If a period is selected for which no data is available, *WinRoute* offers another period where data for the requested statistics might be found.

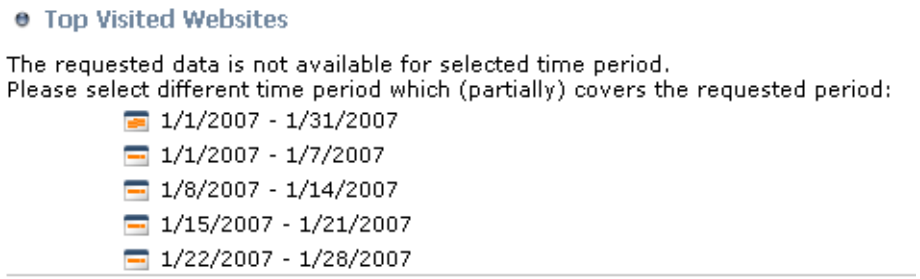

Top Visited Websites
The requested data is not available for selected time period.
Please select different time period which (partially) covers the requested period:
1/1/2007 - 1/31/2007
1/1/2007 - 1/7/2007
1/8/2007 - 1/14/2007
1/15/2007 - 1/21/2007
1/22/2007 - 1/28/2007

Figure 19.11 Selection of a new time period for website statistics

19.6 User statistics

The *Individual* tab allows showing of statistics for a selected user.

First, select a user in the *Select User* menu. The menu includes all users for which any statistic data is available in the database — i.e. users which were active in the selected period (see chapter 19.2).

Figure 19.12 Selection of a user

TIP: The way of users' names are displayed in the *Select User* menu can be set in the *Administration Console*, in section *Accounting*, after clicking on the *Advanced* button (see chapter 19.2).

When a user is selected, full name, username and email address are displayed (if defined in the user account). The same type of statistics as total statistics in the *Individual* section will be shown for the user, as follows:

- volume of data transferred in individual subperiods of the selected accounting period,
- top visited websites,

- top requested web categories,
- used protocols and their part in the total volume of transferred data,

For detail information on individual statistic sections, see chapter 19.5.

19.7 Users by Traffic

The *Users by Traffic* section shows table of all users sorted by volume of transferred data. The table provides an information of part of the user in the total volume of the transferred data.

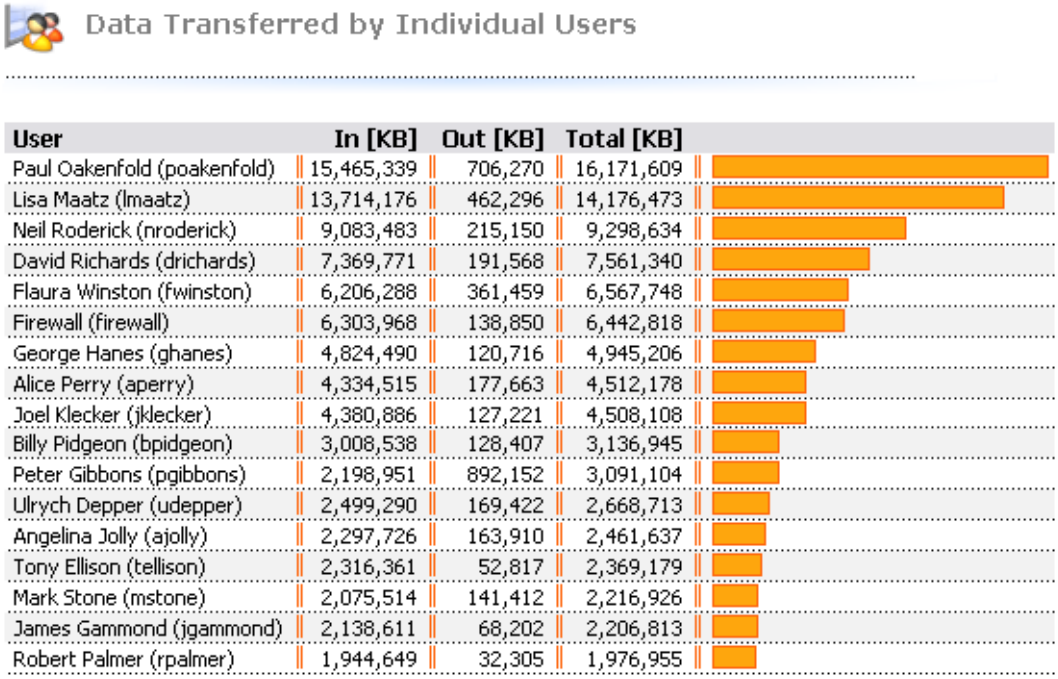

Data Transferred by Individual Users
User
In [KB]
Out [KB]
Total [KB]
Paul Oakenfold (poakenfold) 15,465,339 706,270 16,171,609
Lisa Maatz (lmaatz) 13,714,176 462,296 14,176,473
Neil Roderick (nroderick) 9,083,483 215,150 9,298,634
David Richards (drichards) 7,369,771 191,568 7,561,340
Flaura Winston (fwinston) 6,206,288 361,459 6,567,748
Firewall (firewall) 6,303,968 138,850 6,442,818
George Hanes (ghanes) 4,824,490 120,716 4,945,206
Alice Perry (aperry) 4,334,515 177,663 4,512,178
Joel Klecker (jklecker) 4,380,886 127,221 4,508,108
Billy Pidgeon (bpidgeon) 3,008,538 128,407 3,136,945
Peter Gibbons (pgibbons) 2,198,951 892,152 3,091,104
Ulrych Depper (udepper) 2,499,290 169,422 2,668,713
Angelina Jolly (ajolly) 2,297,726 163,910 2,461,637
Tony Ellison (tellison) 2,316,361 52,817 2,369,179
Mark Stone (mstone) 2,075,514 141,412 2,216,926
James Gammond (jgammond) 2,138,611 68,202 2,206,813
Robert Palmer (rpalmer) 1,944,649 32,305 1,976,955

Figure 19.13 The Users by Traffic table

Each row of the table provides name of the user along with information of data transferred by the user: incoming data (download), outgoing data (upload) and the total volume of transferred data. Click on the name of a user to switch to the *Individual* tab and see detailed statistics of the particular user (see chapter 19.6).

TIP: The way of users' names are displayed in the table can be set in the *Administration Console*, in section *Accounting*, after clicking on the *Advanced* button (see chapter 19.2).

19.8 Top Visited Websites

The *Visited Sites* tab includes statistics for the top ten most frequently visited web domains. These statistics provide for example the following information:

- which sites (domains) are visited by the users regularly,
- which users are the most active in web browsing,

The chart on the left of the tab shows top ten visited web domains. The number in the chart refers to number of visits of all web pages of the particular domain in the selected accounting period.

Note: The *HTTP* protocol inspector "sees" only individual HTTP requests. To count number of visited pages (i.e. to recognize which requests were sent within a single visit), *WinRoute* uses a special heuristic algorithm. The information, therefore, cannot be precise, though the approximation is very good.

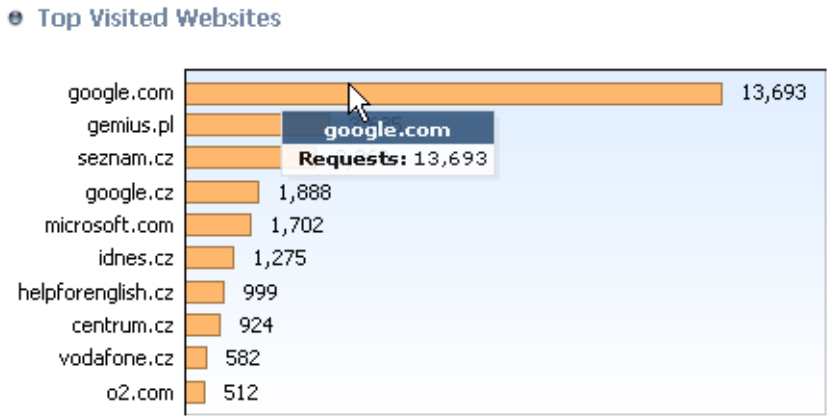
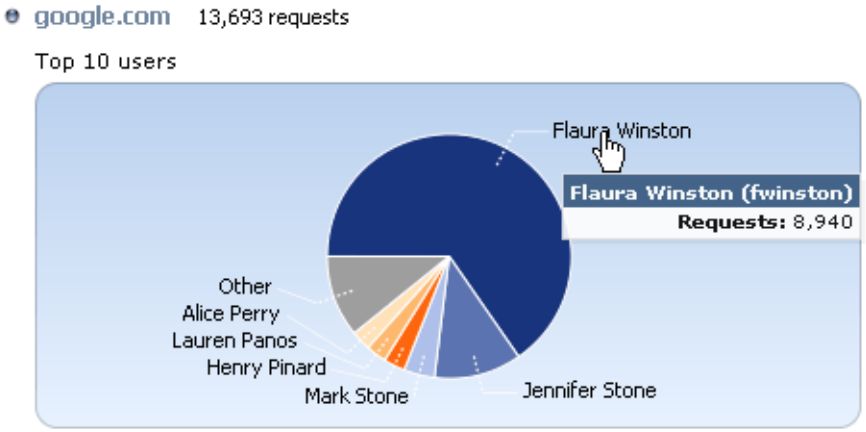


Figure 19.14 Top visited web domains

The right part of the tab shows detailed statistics for each of the top ten visited domains:

- The header provides name of the DNS name and total number of visits at websites on servers belonging to the domain.
- The chart shows part of the most active users (up to six items) in the total visit rate of the particular domain.
- The table below the chart shows the most active users sorted by number of visits at websites within the particular domain (up to ten users). Click on the name of a user in the chart or table to switch to the *Individual* tab and see detailed statistics of the particular user (see chapter 19.6).



User	Requests
Flaura Winston (fwinston)	8,940
Jennifer Stone (jstone)	1,588
Mark Stone (mstone)	560
Henry Pinard (hpinard)	391
Lauren Panos (lpanos)	375
Alice Perry (aperry)	357
Norman Flanders (nflanders)	294
Lisa Maatz (lmaatz)	222
Paul Oakenfold (poakenfold)	144
Ulrych Depper (udepper)	98

Figure 19.15 Top active users for the particular domain

TIP: The way of users' names are displayed in the table can be set in the *Administration Console*, in section *Accounting*, after clicking on the *Advanced* button (see chapter 19.2). Only full names are shown in charts (or usernames if the full name is not defined in the account of the particular user).

19.9 Top Requested Web Categories

The *Web Categories* section includes statistics of the top ten visited web pages categorized by the *ISS OrangeWeb Filter*. Statistics of categories provide more general information of visited websites. For example, the information help figure out how much users browse websites not related to their work issues.

The chart on the left shows the top ten most visited web categories in the selected accounting period. The number in the chart refers to total number of HTTP requests included in the particular category. For technical reasons, it is not possible to recognize whether the number includes requests to a single page or to multiple pages. Therefore, number of requests is usually much higher than number of visits in statistics of the top visited websites (see chapter 19.8).

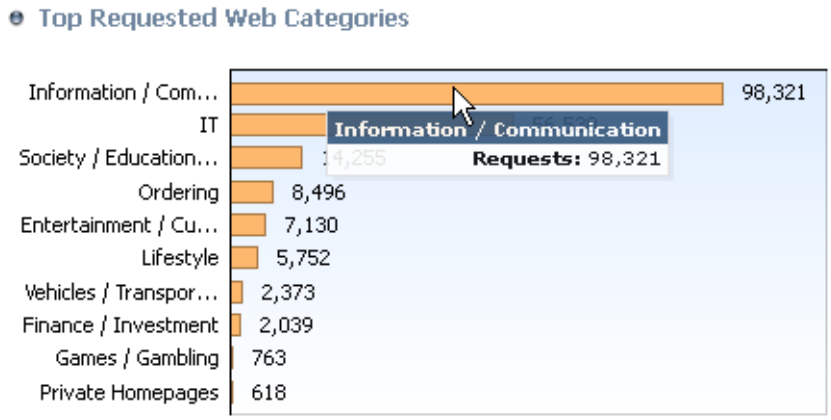
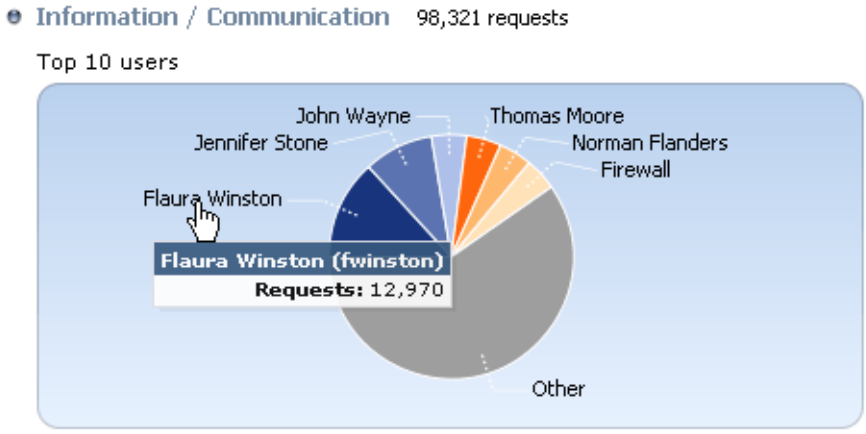


Figure 19.16 Top visited websites sorted by categories

The right section of the tab provides detailed statistics for each of the top ten most frequented web categories:



User	Requests
Flaura Winston (fwinston)	12,970
Jennifer Stone (jstone)	9,064
John Wayne (jwayne)	4,572
Thomas Moore (tmoore)	4,537
Norman Flanders (nflanders)	4,310
Firewall (firewall)	4,240
Alice Perry (aperry)	4,025
George Hanes (ghanes)	3,715
Andrew McKay (amckay)	3,440
Laurette Stilles (lstilles)	2,939

Figure 19.17 Top users for a selected category

- The header provides name of the category and total number of requests to websites belonging to the category.
- The chart shows part of the most active users (up to six items) in the total visit rate of the particular category.
- The table below the chart shows the most active users sorted by number of requests to the particular web category (up to ten users).

  Click on the name of a user in the chart or table to switch to the *Individual* tab and see detailed statistics of the particular user (see chapter 19.6).

  TIP: The way of users' names are displayed in the table can be set in the *Administration Console*, in section *Accounting*, after clicking on the *Advanced* button (see chapter 19.2). Only full names are shown in charts (or usernames if the full name is not defined in the account of the particular user).

Note: Statistics of visited categories might be affected by wrong categorization of some web pages. Some pages might be difficult to categorize for technical reasons and, rarely, it may happen that a website is included in a wrong category. Categorization by *ISS OrangeWeb Filter* is addressed in chapter 10.4.

Chapter 20

Logs

Logs are files where history of certain events performed through or detected by *WinRoute* are recorded and kept. Each log is displayed in a window in the *Logs* section.

Each event is represented by one record line. Each line starts with a time mark in brackets (date and time when the event took place, in seconds). This mark is followed by an information, depending on the log type. If the record includes a URL, it is displayed as a hypertext link. Follow the link to open the page in your default browser.

Optionally, records of each log may be recorded in files on the local disk[7] and/or on the *Syslog* server.

Locally, the logs are saved in the files under the `logs` subdirectory where *WinRoute* is installed. The file names have this pattern:

`file_name.log`

(e.g. `debug.log`). Each log includes an `.idx` file, i.e. an indexing file allowing faster access to the log when displayed in *Administration Console*.

Individual logs can be rotated — after a certain time period or when a threshold of the file size is reached, log files are stored and new events are logged to a new (empty) file.

Administration Console allows to save a selected log (or its part) in a file as plaintext or in HTML. The log saved can be analysed by various tools, published on web servers, etc.

20.1 Log settings

Log parameters (file names, rotation, sending to a *Syslog* server) can be set in the *Configuration* → *Accounting* section. In this section of the guide an overview of all logs used by *WinRoute* are provided.

Double-click on a selected log (or select a log and click on the *Edit* button) to open a dialog where parameters for the log can be set.

Note: If the log is not saved in a file on the disk, only records generated since the last login to *WinRoute Firewall Engine* will be shown in the *Administration Console*. After logout (or closing of *Administration Console*), the records will be lost.

[7] Local disk is a disk of the computer where *WinRoute* is installed, not a computer where *Administration Console* is running!

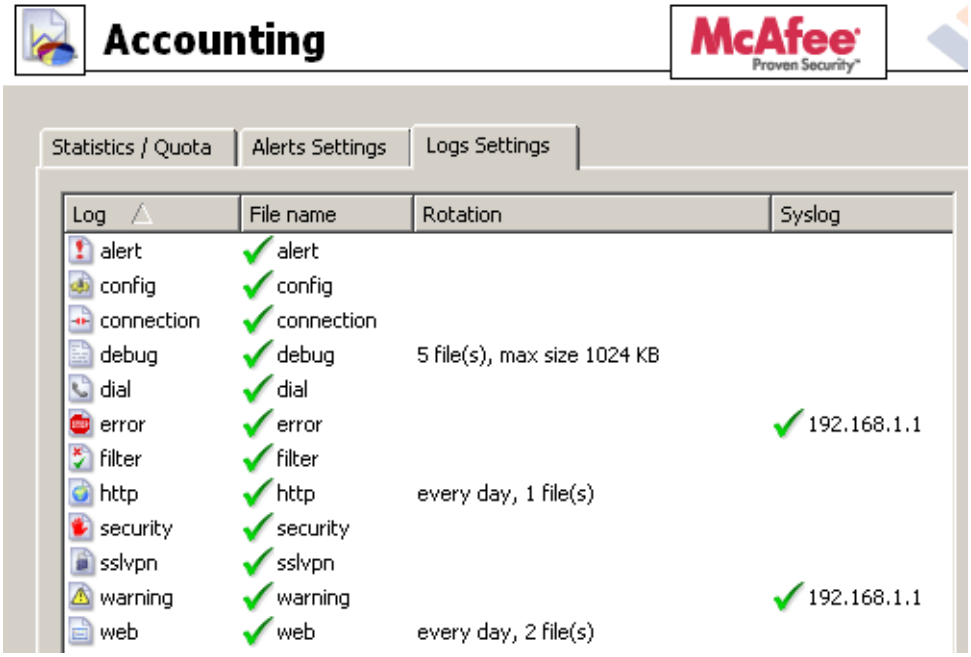


Figure 20.1 Log settings

File Logging

Use the *File Logging*tab to define file name and rotation parameters.

Enable logging to file

Use this option to enable/disable logging to file according to the *File name* entry (the `.log` extension will be appended automatically).

If this option is disabled, none of the following parameters and settings will be available.

Rotate regularly

Set intervals in which the log will be rotated regularly. The file will be stored and a new log file will be started in selected intervals.

Rotate when file exceeds size

Set a maximal size for each file. Whenever the threshold is reached, the file will be rotated. Maximal size is specified in megabytes (MB).

Note: If both *Rotate regularly* and the *Rotate when file exceeds size* are enabled, the particular file will be rotated whenever one of these conditions is met.

Keep at most ... log file(s)

Maximal count of log files that will be stored. Whenever the threshold is reached, the oldest file will be deleted.

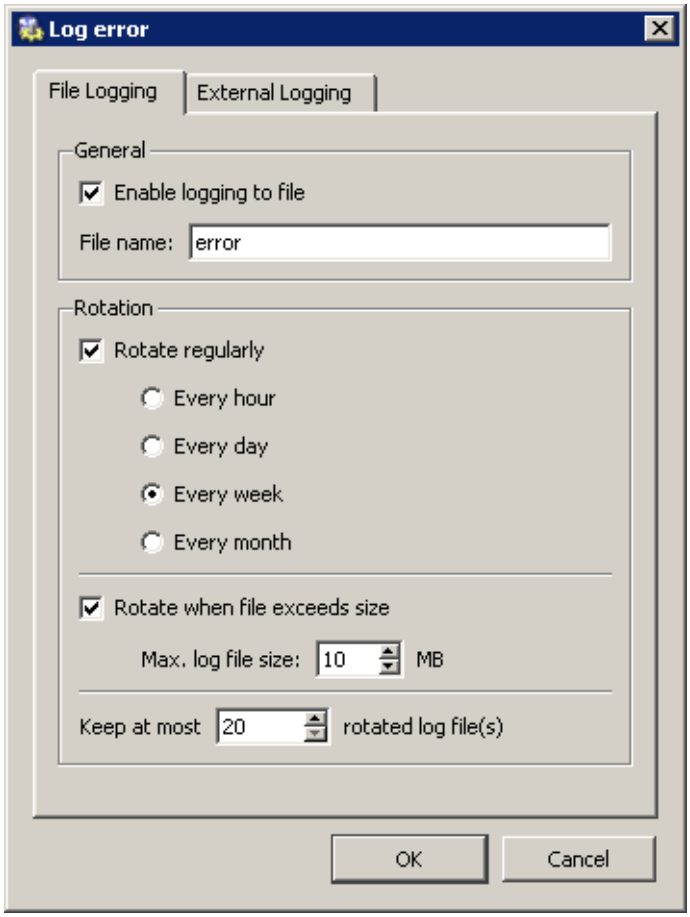


Figure 20.2 File logging settings

Syslog Logging

Parameters for logging to a *Syslog* can be defined in the *External Logging* tab.

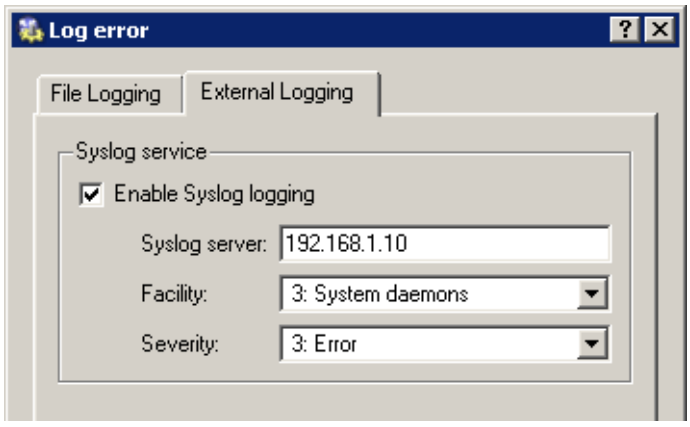


Figure 20.3 Syslog settings

Enable Syslog logging

Enable/disable logging to a *Syslog* server.

If this option is disabled, none of the following parameters and settings will be available.

Syslog server

DNS name or IP address of the *Syslog* server.

Facility

Facility that will be used for the particular *WinRoute* log (depends on the *Syslog* server).

Severity

Severity of logged events (depends on the *Syslog* server).

20.2 Logs Context Menu

When you right-click inside any log window, a context menu will be displayed where you can choose several functions or change the log's parameters (view, logged information).

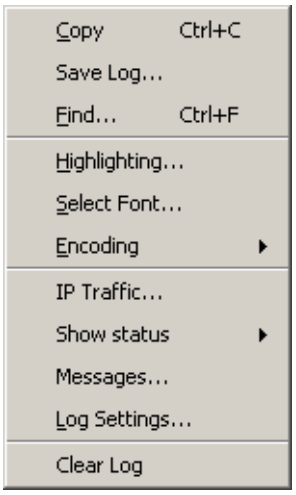


Figure 20.4 Logs Context Menu

Copy

Copies the selected text onto the clipboard. A key shortcut from the operating system can be used (*Ctrl+C* or *Ctrl+Insert* in Windows).

Save log

This option saves the log or selected text in a file as plaintext or in HTML.

TIP: This function provides more comfortable operations with log files than a direct access to log files on the disk of the computer where *WinRoute* is installed. Logs can be saved even if *WinRoute* is administered remotely.

The *Save log* option opens a dialog box where the following optional parameters can be set:

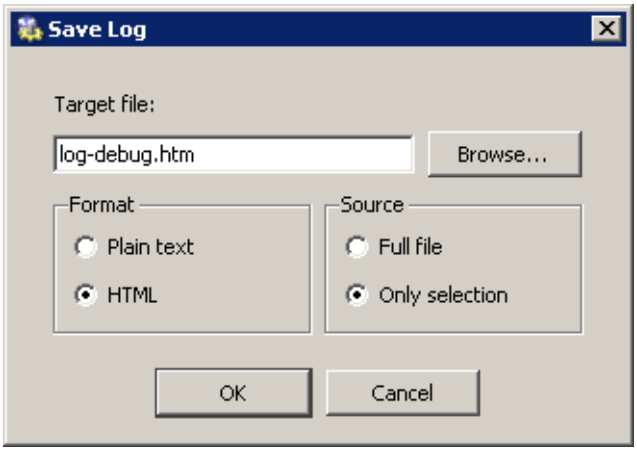


Figure 20.5 Saving a log to a file

- *Target file* — name of the file where the log will be saved. By default, a name derived from the file name is set. The file extension is set automatically in accordance with the format selected.
- *Format* — logs can be saved as plaintext or in HTML. If the HTML format is used, colors will be saved for the lines background (see section *Highlighting*) and all URLs will be saved as hypertext links.
- *Source* — either the entire log or only a part of the text selected can be saved. Bear in mind that in case of remote administration, saving of an entire log may take some time.

Find

Use this option to search for a string in the log. Logs can be scanned either *Up* (search for older events) or *Down* (search for newer events) from the current position.

During the first lookup (when switched to the log window), the log is searched through from the top (or the end, depending on the lookup direction set). Further search starts from the marked text (marked by mouse or as a result of the recent search).

Highlighting

Highlighting may be set for logs meeting certain criteria (for details, see below).

Select font

Within this dialog you can select a font of the log printout. All fonts installed on the host with the *Administration Console* are available.

Encoding

Coding that will be used for the log printout in *Administration Console* can be selected in this section. *UTF-8* is used by default.
HINT: Select a new encoding type if special characters are not printed correctly in non-English versions.

Log debug

A dialog where log parameters such as log file name, rotation and *Syslog* parameters can be set. These parameters can also be set in the *Log settings* tab under *Configuration* → *Accounting*. For details, refer to chapter 20.1.

Clear log

Removes entire log. The file will be removed (not only the information saved in the selected window).
Warning: Removed logs cannot be refreshed anymore.

Note: If a user with read rights only is connected to *WinRoute*(see chapter 13.1), the *Log settings* and *Clear log* options are missing in the log context menu. Only users with full rights can access these functions.

Log highlighting

For better reference, it is possible to set highlighting for logs meeting certain criteria. Highlighting is defined by special rules shared by all logs. Seven colors are available (plus the background color of unhighlighted lines), however, number of rules is not limited.

Use the *Highlighting* option in the context pop-up menu of the corresponding log to set highlighting parameters.

Highlighting rules are ordered in a list. The list is processed from the top. The first rule meeting the criteria stops other processing and the found rule is highlighted by the particular color. Thanks to these features, it is possible to create even more complex combinations of rules, exceptions, etc. In addition to this, each rule can be "disabled" or "enabled" for as long as necessary.

Use the *Add* or the *Edit* button to (re)define a highlighting rule.

Each highlighting rule consists of a condition and a color which will be used to highlight lines meeting the condition. Condition can be specified by a substring (all lines containing the string will be highlighted) or by a so called regular expression (all lines containing one or multiple strings matching the regular expression will be highlighted).

The *Description* item is used for reference only. It is recommended to describe all created rules well (it is recommended to mention also the name of the log to which the rule applies).

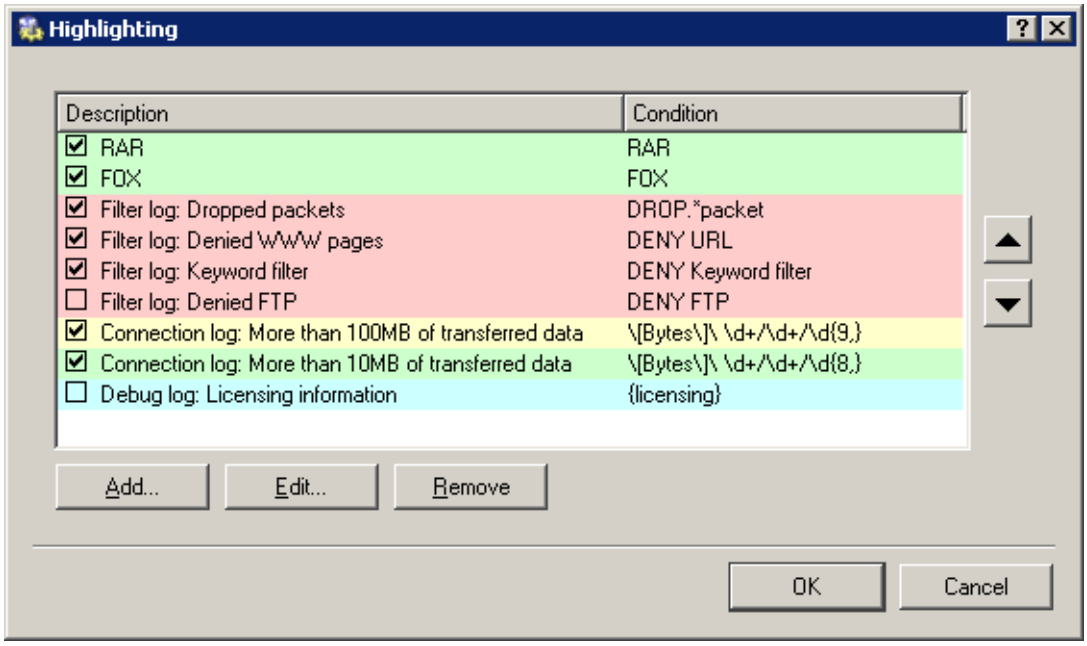


Figure 20.6 Log highlighting settings

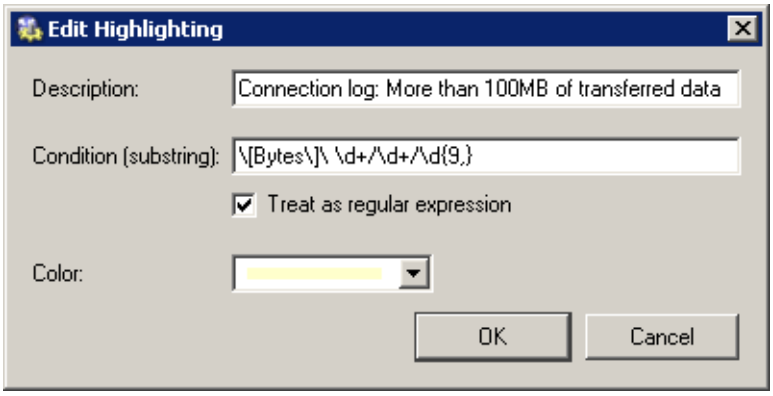


Figure 20.7 Highlighting rule definition

Note: Regular expression is such expression which allows special symbols for string definition. *WinRoute* accepts all regular expressions in accordance with the POSIX standard.

For detailed instructions contact Kerio technical support. For detailed information, refer for example to

`http://www.gnu.org/software/grep/`

The Debug log advanced settings

Special options are available in the *Debug* log context menu. These options are available only to users with full administration rights (see chapter 13.1)..

IP Traffic

This function enables monitoring of packets according to the user defined log expression.

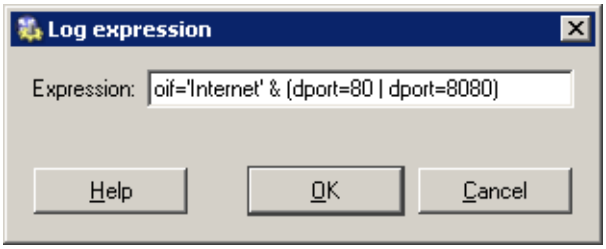


Figure 20.8 Expression for traffic monitored in the debug log

The expression must be defined with special symbols. After clicking on the *Help* button, a brief description of possible conditions and examples of their use will be displayed.

Logging of IP traffic can be cancelled by leaving or setting the *Expression* entry blank.

Show status

A single overview of status information regarding certain *WinRoute* components. This information can be helpful especially when solving problems with *Kerio Technologies* technical support.

Messages

This option enables the administrator to define advanced settings for information that will be monitored in the *Debug* log: This information may be helpful when solving issues regarding *WinRoute* components and/or certain network services.

- *WAN / Dial-up messages* information about dialed lines (request dialing, auto disconnection down-counter),
- *WinRoute services* — protocols processed by *WinRoute* services (*DHCP server* and *DNS Forwarder*),
- *Decoded protocols* — displays message content of all selected protocols that use *WinRoute* modules (HTTP and DNS)
- *Miscellaneous* — more information, such as information about removed packets, packets with errors, HTTP cache, user authentication, processing packets by the *Bandwidth Limiter* module, etc.
- *Developers logging* — detailed logs for debugging (can be used especially when solving issues with assistence of the *Kerio Technologies* technical support),
- *Kerio VPN* — detailed information on traffic within *Kerio VPN* — VPN tunnels, VPN clients, encryptions, exchange of routing information, web server for

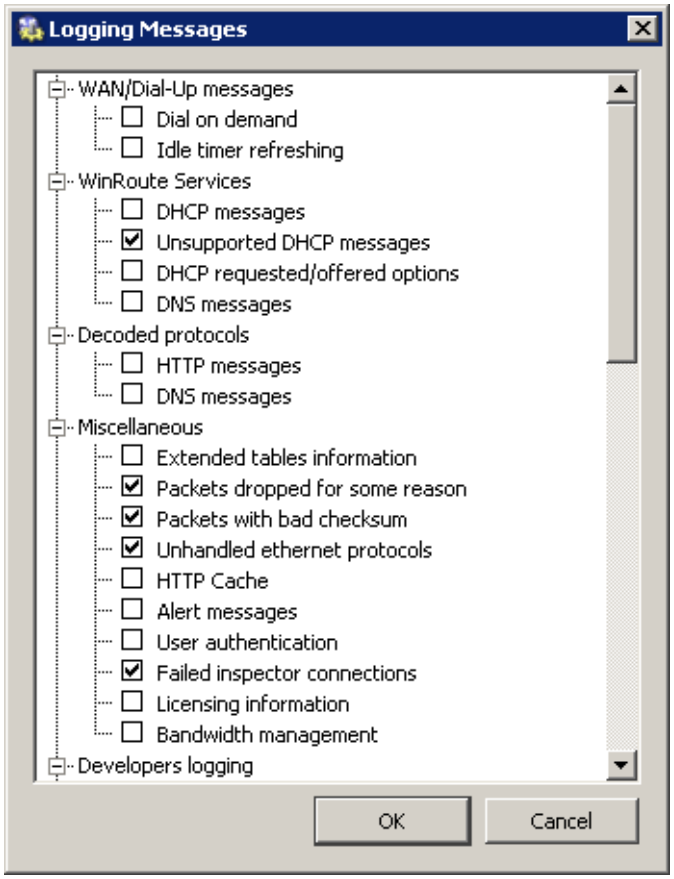


Figure 20.9 Selection of information monitored by the Debug log

Clientless SSL-VPN, etc.

20.3 Alert Log

The *Alert* log provides a complete history of alerts generated by *WinRoute* (e.g. alerts upon virus detection, dialing and hanging-up, reached quotas, detection of P2P networks, etc.).

Each event in the *Alert* log includes a time stamp (date and time when the event was logged) and information about an alert type (in capitals). The other items depend on an alert type.

HINT: Email and SMS alerts can be set under *Configuration* → *Accounting*. All sent alerts can be viewed in the *Status* → *Alert messages* section (for details, see chapter 17.3).

20.4 Config Log

The *Config* log stores a complete communication history between *Administration Console* and the *WinRoute Firewall Engine* — the log allows you to find out what administration actions were performed by which user, and when.

The *Config* window contains three log types:

1. *Information about user logins/logouts to/from the WinRoute's administration*

   Example:

   ```
   [18/Apr/2003 10:25:02] james - session opened
     for host 192.168.32.100
   [18/Apr/2003 10:32:56] james - session closed
     for host 192.168.32.100
   ```

   - `[18/Apr/2003 10:25:02]` — date and time when the record was written to the log
   - `jsmith` — the login name of the user logged in the *WinRoute* administration
   - `session opened for host 192.168.32.100` — information about the beginning of the communication and the IP address of the computer from which the user connected
   - `session closed for host 192.168.32.100` — information about the end of the communication with the particular computer (user logout or *Administration Console* closed)

2. *Configuration database changes*

   Changes performed in the *Administration Console*. A simplified form of the SQL language is used when communicating with the database.

   Example:

   ```
   [18/Apr/2003 10:27:46] jsmith - insert StaticRoutes
     set Enabled='1', Description='VPN',
     Net='192.168.76.0', Mask='255.255.255.0',
     Gateway='192.168.1.16', Interface='LAN', Metric='1'
   ```

   - `[18/Apr/2003 10:27:46]` — date and time when the record was written
   - `jsmith` — the login name of the user logged in the *WinRoute* administration

- `insert StaticRoutes ...` — the particular command used to modify the *WinRoute's* configuration database (in this case, a static route was added to the routing table)

3. *Other changes in configuration*

   A typical example of this record type is the change of traffic rules. When the user hits *Apply* in *Configuration* → *Traffic policy*, a complete list of current traffic rules is written to the *Config* log.

   Example:

   ```
   [18/Apr/2003 12:06:03] Admin - New traffic policy set:
   [18/Apr/2003 12:06:03] Admin - 1: name=(ICMP Traffic)
     src=(any) dst=(any) service=("Ping")
     snat=(any) dnat=(any) action=(Permit)
     time_range=(always) inspector=(default)
   ```

   - `[18/Apr/2003 12:06:03]` — date and time of the change
   - `Admin` — login name of the user who did the change
   - `1:` — traffic rule number (rules are numbered top to bottom according to their position in the table, the numbering starts from 1)
   - `name=(ICMP Traffic) ...` — traffic rule definition (name, source, destination, service etc.)

   Note: The default rule (see chapter 6.1) is marked with `default` instead of the positional number.

20.5 Connection Log

Connection logs for traffic rules which are configured to be logged using the *Log matching connections* option (refer to chapter 66).

How to read the Connection Log?

```
[18/Apr/2003 10:22:47] [ID] 613181 [Rule] NAT
  [Service] HTTP [User] james
  [Connection] TCP 192.168.1.140:1193 -> hit.top.com:80
  [Duration] 121 sec [Bytes] 1575/1290/2865 [Packets] 5/9/14
```

- `[18/Apr/2003 10:22:47]` — date and time when the event was logged (Note: Connection logs are saved immediately after a disconnection)
- `[ID] 613181` — *WinRoute* connection identification number

- `[Rule] NAT` — name of the traffic rule which has been used (a rule by which the traffic was allowed or denied).
- `[Service] HTTP` — name of a corresponding application layer service (recognized by destination port).

  If the corresponding service is not defined in *WinRoute* (refer to chapter 12.3), the `[Service]` item is missing in the log.
- `[User] james` name of the user connected to the firewall from a host which participates in the traffic.

  If no user is currently connected from the corresponding host, the `[User]` item is missing in the log.
- `[Connection] TCP 192.168.1.140:1193 -> hit.top.com:80` — protocol, source IP address and port, destination IP address and port. If an appropriate log is found in the *DNS Forwarder* cache (see chapter 5.3), the host's DNS name is displayed instead of its IP address. If the log is not found in the cache, the name is not detected (such DNS requests would slow *WinRoute* down).
- `[Duration] 121 sec` — duration of the connection (in seconds)
- `[Bytes] 1575/1290/2865` — number of bytes transferred during this connection (transmitted /accepted /total).
- `[Packets] 5/9/14` — number of packets transferred through this connection (transmitted/accepted/total).

20.6 Debug Log

Debug (debug information) is a special log which can be used to monitor certain kinds of information, especially for problem-solving. Too much information could be confusing and impractical if displayed all at the same time. Usually, you only need to display information relating to a particular service or function. In addition, displaying too much information slows *WinRoute's* performance. Therefore, it is strongly recommended to monitor an essential part of information and during the shortest possible period only.

20.7 Dial Log

Data about dialing and hanging up the dial-up lines, and about time spent on-line.

The following items (events) can be reported in the *Dial* log:

1. Manual connection (from the *Administration Console* — see chapter 5.1 or right from the operating system)

```
[15/Mar/2004 15:09:27] Line "Connection" dialing,
  console 127.0.0.1 - Admin
[15/Mar/2004 15:09:39] Line "Connection" successfully connected
```

The first log item is reported upon initialization of dialing. The log always includes *WinRoute* name of the dialed line (see chapter 5.1). If the line is dialed from the *Administration Console*, the log provides this additional information

- where the line was dialed from (`console` — *Administration Console*,
- IP address of the client (i.e. IP address of the *Administration Console*),
- login name of the user who sent the dial request.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

2. Line disconnection (manual or automatic, performed after a certain period of idleness)

```
[15/Mar/2004 15:29:18] Line "Connection" hang-up,
  console 127.0.0.1 - Admin
[15/Mar/2004 15:29:20] Line "Connection" disconnected,
  connection time 00:15:53, 1142391 bytes received,
  250404 bytes transmitted
```

The first log item is recorded upon reception of a hang-up request. The log provides information about interface name, client type, IP address and username.

The second event is logged upon a successful hang-up. The log provides information about interface name, time of connection (`connection time`), volume of incoming and outgoing data in bytes (`bytes received` and `bytes transmitted`).

3. Disconnection caused by an error (connection is dropped)

```
[15/Mar/2004 15:42:51] Line "Connection" dropped,
  connection time 00:17:07, 1519 bytes received,
  2504 bytes transmitted
```

The items are the same as in the previous case (the second item — the `disconnected` report).

4. Requested dialing (as a response to a DNS query)

```
[15/Mar/2004 15:51:27] DNS query for "www.microcom.com"
  (packet UDP 192.168.1.2:4567 -> 195.146.100.100:53)
  initiated dialing of line "Connection"
[15/Mar/2004 15:51:38] Line "Connection" successfully connected
```

The first log item is recorded upon reception of a DNS request (the *DNS forwarder* has not found requested DNS record in its cache). The log provides:

- DNS name from which IP address is being resolved,
- description of the packet with the corresponding DNS query (protocol, source IP address, source port, destination IP address, destination port),
- name of the line to be dialed.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

5. On-demand dialing (response to a packet sent from the local network)

```
[15/Mar/2004 15:53:42] Packet
  TCP 192.168.1.3:8580 -> 212.20.100.40:80
  initiated dialing of line "Connection"
[15/Mar/2004 15:53:53] Line "Connection" successfully connected
```

The first record is logged when *WinRoute* finds out that the route of the packet does not exist in the routing table. The log provides:

- description of the packet (protocol, source IP address, destination port, destination IP address, destination port),
- name of the line to be dialed.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

6. Connection error (e.g. error at the modem was detected, dial-up was disconnected, etc.)

```
[15/Mar/2004 15:59:08] DNS query for "www.microsoft.com"
  (packet UDP 192.168.1.2:4579 -> 195.146.100.100:53)
  initiated dialing of line "Connection"
[15/Mar/2004 15:59:12] Line "Connection" disconnected
```

The first record represents a DNS record sent from the local network, from that the line is to be dialed (see above).

The second log item (immediately after the first one) informs that the line has been hung-up. Unlike in case of a regular disconnection, time of connection and volume of transmitted data are not provided (because the line has not been connected).

20.8 Error Log

The *Error* log displays information about serious errors that affect the functionality of the entire firewall. *WinRoute* administrator should check this log regularly and fix detected problems as soon as possible. Otherwise, users might have problems with some services or/and serious security problems might arise.

A typical error message in the *Error* log could be: a problem when starting a service (usually a collision at a particular port number), problems when writing to the disk or when initializing anti-virus, etc.

Each record in the *Error* log contains error code and sub-code as two numbers in parentheses `(x y)`. The error code (`x`) may fall into one of the following categories:

- `1-999` — system resources problem (insufficient memory, memory allocation error, etc.)
- `1000-1999` — internal errors (unable to read routing table or interface IP addresses, etc.)
- `2000-2999` — license problems (license expired, the number of users would break license limit, unable to find license file, etc.)
- `3000-3999` — configuration errors (unable to read configuration file, detected a look in the configuration of *DNS Forwarder* or the *Proxy server*, etc.)
- `4000-4999` — network (socket) errors
- `5000-5999` — errors while starting or stopping the *WinRoute Firewall Engine* (problems with low-level driver, problems when initializing system libraries, services, configuration databases, etc.)
- `6000-6999` — filesystem errors (cannot open /save /delete file)
- `7000-7999` — SSL errors (problems with keys and certificates, etc.)
- `8000-8099` — HTTP cache errors (errors when reading / writing cache files, not enough space for cache, etc.)
- `8100-8199` — errors of the *ISS OrangeWeb Filter* module
- `8200-8299` — authentication subsystem errors
- `8300-8399` — anti-virus module errors (anti-virus test not successful, problems when storing temporary files, etc.)

- `8400–8499` — dial-up error (unable to read defined dial-up connections, line configuration error, etc.)
- `8500–8599` — LDAP errors (server not found, login failed, etc.)

Note: If you are not able to correct an error (or figure out what it is caused by) which is repeatedly reported in the *Error* log, do not hesitate to contact our technical support. For detailed information, refer to chapter 25 or to `http://www.kerio.com/`.

20.9 Filter Log

This log contains information about web pages and objects blocked by the HTTP and FTP filters (see chapters 10.2 and 10.6) and about packets blocked by traffic rules if packet logging is enabled for the particular rule (see chapter 6 for more information). Each log line includes the following information depending on the component which generated the log:

- when an HTTP or FTP rule is applied: rule name, user, IP address of the host which sent the request, object's URL
- when a traffic rule is applied: detailed information about the packet that matches the rule (rule name, source and destination address, ports, size, etc.)

Example of a URL rule log message:

```
[18/Apr/2003 13:39:45] ALLOW URL 'McAfee update'
  192.168.64.142 james HTTP GET
  http://update.kerio.com/nai-antivirus/datfiles/4.x/dat-4258.zip
```

- `[18/Apr/2003 13:39:45]` — date and time when the event was logged
- `ALLOW` — action that was executed (`ALLOW` = access allowed, `DENY` = access denied)
- `URL` — rule type (for URL or FTP)
- `'McAfee update'` — rule name
- `192.168.64.142` — IP address of the client
- `jsmith` — name of the user authenticated on the firewall (no name is listed unless at least one user is logged in from the particular host)
- `HTTP GET` — HTTP method used in the request
- `http:// ...` — requested URL

Example of a traffic rule log message:

```
[16/Apr/2003 10:51:00] PERMIT 'Local traffic' packet to LAN,
  proto:TCP, len:47, ip/port:195.39.55.4:41272 ->
  192.168.1.11:3663, flags: ACK PSH , seq:1099972190
  ack:3795090926, win:64036, tcplen:7
```

- `[16/Apr/2003 10:51:00]` — date and time when the event was logged
- `PERMIT` — action that was executed with the packet (`PERMIT`, `DENY` or `DROP`)
- `Local traffic` —the name of the traffic rule that was applied
- `packet to` — packet direction (either `to` or `from` a particular interface)
- `LAN` — interface name (see chapter 5.1 for details)
- `proto:` — transport protocol (TCP, UDP, etc.)
- `len:` — packet size in bytes (including the headers) in bytes
- `ip/port:` — source IP address, source port, destination IP address and destination port
- `flags:` — TCP flags
- `seq:` — sequence number of the packet (TCP only)
- `ack:` — acknowledgement sequence number (TCP only)
- `win:` — size of the receive window in bytes (it is used for data flow control — TCP only)
- `tcplen:` — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

20.10 Http log

This log contains all HTTP requests that were processed by the HTTP inspection module (see section 12.3) or by the built-in proxy server (see section 5.5). The log has the standard format of either the *Apache* WWW server (see `http://www.apache.org/`) or of the *Squid* proxy server (see `http://www.squid-cache.org/`). The enable or disable the *Http* log, or to choose its format, go to*Configuration* → *Content Filtering* → *HTTP Policy* (refer to section 10.2 for details).

Notes:

1. Only accesses to allowed pages are recorded in the *HTTP* log. Request that were blocked by HTTP rules are logged to the *Filter* log (see chapter 20.9), if the *Log* option is enabled in the particular rule (see section 10.2).

2. The *Http* log is intended to be processes by external analytical tools. The *Web* log (see bellow) is better suited to be viewed by the *WinRoute* administrator.

An example of Http log record that follows the Apache format:

```
[18/Apr/2003 15:07:17] 192.168.64.64 - rgabriel
  [18/Apr/2003:15:07:17 +0200]
  "GET http://www.kerio.com/ HTTP/1.1" 304 0 +4
```

- `[18/Apr/2003 15:07:17]` — date and time when the event was logged
- `192.168.64.64` — IP address of the client host
- `rgabriel` — name of the user authenticated through the firewall (a dash is displayed if no user is authenticated through the client)
- `[18/Apr/2003:15:07:17 +0200]` — date and time of the HTTP request. The `+0200` value represents time difference from the UTC standard (+2 hours are used in this example — CET).
- `GET` — used HTTP method
- `http://www.kerio.com` — requested URL
- `HTTP/1.1` — version of the HTTP protocol
- `304` — return code of the HTTP protocol
- `0` — size of the transferred object (file) in bytes
- `+4` — count of HTTP requests transferred through the connection

An example of Http log record that follows the Squid format:

```
1058444114.733 0 192.168.64.64 TCP_MISS/304 0
  GET http://www.squid-cache.org/ - DIRECT/206.168.0.9
```

- `1058444114.733` — timestamp (seconds and miliseconds since January 1st, 1970)
- `0` — download duration (not measured in *WinRoute*, always set to zero)

- `192.168.64.64` — IP address of the client (i.e. of the host from which the client is connected to the website)
- `TCP_MISS` — the TCP protocol was used and the particular object was not found in the cache ("missed"). *WinRoute* always uses this value for this field.
- `304` — return code of the HTTP protocol
- `0` — transferred data amount in bytes (HTTP object size)
- `GET http://www.squid-cache.org/` — the HTTP request (HTTP method and URL of the object)
- `DIRECT` — the WWW server access method (*WinRoute* always uses `DIRECT` access)
- `206.168.0.9` — IP address of the WWW server

20.11 Security Log

A log for security-related messages. Records of the following types may appear in the log:

1. *Anti-spoofing log records*

   Messages about packets that where captured by the *Anti-spoofing* module (packets with invalid source IP address — see section 15.2 for details)

   Example:

   ```
   [17/Jul/2003 11:46:38] Anti-Spoofing:
     Packet from LAN, proto:TCP, len:48,
     ip/port:61.173.81.166:1864 -> 195.39.55.10:445,
     flags: SYN , seq:3819654104 ack:0, win:16384, tcplen:0
   ```

   - `packet from` — packet direction (either `from`, i.e. sent via the interface, or `to`, i.e. received via the interface)
   - `LAN` — interface name (see chapter 5.1 for details)
   - `proto:` — transport protocol (TCP, UDP, etc.)
   - `len:` — packet size in bytes (including the headers) in bytes
   - `ip/port:` — source IP address, source port, destination IP address and destination port

- `flags:` — TCP flags
- `seq:` — sequence number of the packet (TCP only)
- `ack:` — acknowledgement sequence number (TCP only)
- `win:` — size of the receive window in bytes (it is used for data flow control — TCP only)
- `tcplen:` — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

2. *FTP protocol parser log records*

   Example 1:

   ```
   [17/Jul/2003 11:55:14] FTP: Bounce attack: attempt:
     client: 1.2.3.4, server: 5.6.7.8,
     command: PORT 10,11,12,13,14,15
   ```

   (attack attempt detected — a foreign IP address in the `PORT` command)

   Example 2:

   ```
   [17/Jul/2003 11:56:27] FTP: Malicious server reply:
     client: 1.2.3.4, server: 5.6.7.8,
     response: 227 Entering Passive Mode (10,11,12,13,14,15)
   ```

   (suspicious server reply with a foreign IP address)

3. *Failed user authentication log records*

   Message format:

   `Authentication: <service>: Client: <IP address>: <reason>`

   - `<service>` — The *WinRoute* service to which the user attempted to authenticate (`Admin` = administration using *Kerio Administration Console*, `WebAdmin` = web administration interface, `WebAdmin SSL` = secure web administration interface, `Proxy` = proxy server user authentication)
   - `<IP address>` — IP address of the computer from which the user attempted to authenticate
   - `<reason>` — reason of the authentication failure (nonexistent user / wrong password)

   Note: For detailed information on user quotas, refer to chapters 13.1 and 8.1.

4. Information about the start and shutdown of the WinRoute Firewall Engine

a) Engine Startup:

```
[17/Dec/2004 12:11:33] Engine:  Startup.
```

b) Engine Shutdown:

```
[17/Dec/2004 12:22:43] Engine:  Shutdown.
```

20.12 Sslvpn Log

In this log, operations performed in the *Clientless SSL-VPN* interface are recorded. Each log line provides information about an operation type, name of the user who performed it and file associated with the operation.

Example:

```
[17/Mar/2005 08:01:51] Copy File: User: jsmith@company.com
  File: '\\server\data\www\index.html'
```

20.13 Warning Log

The *Warning* log displays warning messages about errors of little significance. Warnings can display for example reports about invalid user login (invalid username or password), error in communication of the server and Web administration interface, etc.

Events recalling warning messages in this log do not seriously affect *WinRoute* functionality. However, they can point at current or possible problems. The *Warning* log can help if for example a user is complaining that certain services are not working.

Each warning message is identified by its numerical code (`code xxx:`). The following warning categories are defined:

- `1000-1999` — system warnings (e.g. an application found that is known as conflicting)
- `2000-2999` — *WinRoute* configuration problems (e.g. HTTP rules require user authentication, but the WWW interface is not enabled)
- `3000-3999` — warning from individual *WinRoute* modules (e.g. DHCP server, anti-virus check, etc.)
- `4000-4999` — license warnings (subscription expiration, forthcoming expiration of *WinRoute's* license, *ISS OrangeWeb Filter* license, or the *McAfee* anti-virus license)

  Note: License expiration is considered to be an error and it is logged into the *Error* log.

Examples of Warning logs:

```
[15/Apr/2004 15:00:51] (3004) Authentication subsystem warning:
  Kerberos 5 auth: user john@company.com not authenticated
[15/Apr/2004 15:00:51] (3004) Authentication subsystem warning:
  Invalid password for user admin
[16/Apr/2004 10:53:20] (3004) Authentication subsystem warning:
  User jsmith doesn't exist
```

- The first log informs that authentication of user `jsmith` by the *Kerberos* system in the `company.com` domain failed
- The second log informs on a failed authentication attempt by user `admin` (invalid password)
- The third log informs on an authentication attempt by a user which does not exist (`johnblue`)

Note: With the above three examples, the relevant records will also appear in the `Security` log.

20.14 Web Log

This log contains all HTTP requests that were processed by the HTTP inspection module (see section 12.3) or by the built-in proxy server (see section 5.5). Unlike in the *HTTP* log, the *Web* log displays only the title of a page and the *WinRoute* user or the IP host viewing the page. In addition to each URL, name of the page is provided for better reference.

For administrators, the *Web* log is easy to read and it provides the possibility to monitor which Websites were opened by each user.

How to read the Web Log?

```
[24/Apr/2003 10:29:51] 192.168.44.128 james
  "Kerio Technologies | No Pasaran!" http://www.kerio.com/
```

- `[24/Apr/2003 10:29:51]` — date and time when the event was logged
- `192.168.44.128` — IP address of the client host
- `james` — name of authenticated user (if no user is authenticated through the client host, the name is substituted by a dash)
- `"Kerio Technologies | No Pasaran!"` — page title

  (content of the `<title>` HTML tag)

Note: If the page title cannot be identified (i.e. for its content is compressed), the "Encoded content" will be reported

- http://www.kerio.com/ — URL pages

Chapter 21

Kerio VPN

WinRoute enables secure interconnection of remote private networks using an encrypted tunnel and it provides clients secure access to their local networks via the Internet. This method of interconnection of networks (and of access of remote clients to local networks) is called virtual private network (*VPN*). *WinRoute* includes a proprietary implementation of VPN, called "*Kerio VPN*".

Kerio VPN is designed so that it can be used simultaneously with the firewall and with NAT (even along with multiple translations). Creation of an encrypted tunnel between networks and setting remote access of clients at the server is very easy.

Kerio VPN enables creation of any number of encrypted *server-to-server* connections (i.e. tunnels to remote private networks). Tunnels are created between two *WinRoutes* (typically at Internet gateways of corresponding networks). Individual servers (endpoints of the tunnels) verify each other using SSL certificates — this ensures that tunnels will be created between trustworthy servers only.

Individual hosts can also connect to the VPN server in *WinRoute* (secured *client-to-server* connections). Identities of individual clients are authenticated against a username and password (transmitted also by secured connection), so that unauthorized clients cannot connect to local networks.

Remote connections of clients are performed through *Kerio VPN Client*, included in *WinRoute* (for a detailed description, view the stand-alone *Kerio VPN Client — User Guide* document).

Note: For deployment of the *Kerio VPN*, it is supposed that *WinRoute* is installed at a host which is used as an Internet gateway. If this condition is not met, *Kerio VPN* can also be used, but the configuration can be quite complicated.

Benefits of Kerio VPN

In comparison with other products providing secure interconnection of networks via the Internet, the *Kerio VPN* solution provides several benefits and additional features.

- Easy configuration (only a few basic parameters are required for creation of tunnels and for configuration of servers which clients will connect to).
- No additional software is required for creation of new tunnels (*Kerio VPN Client* must be installed at remote clients — installation file of the application is 4 MB).

- No collisions arise while encrypted channels through the firewall are being created. It is supposed that one or multiple firewalls (with or without NAT) are used between connected networks (or between remote clients and local networks).
- No special user accounts must be created for VPN clients. User accounts in *WinRoute* (or domain accounts if the *Active Directory* is used — see chapter 8.1) are used for authentication.
- Statistics about VPN tunnels and VPN clients can be viewed in *WinRoute* (refer to chapter 18.1).

21.1 VPN Server Configuration

VPN server is used for connection of remote endpoints of VPN tunnels and of remote clients using *Kerio VPN Client*.

Note: Connection to the VPN server from the Internet must be first allowed by traffic rules. For details, refer to chapters 21.2 and 21.3.

VPN server is available in the *Interfaces* tab of the *Configuration* → *Interfaces* section as a special interface.

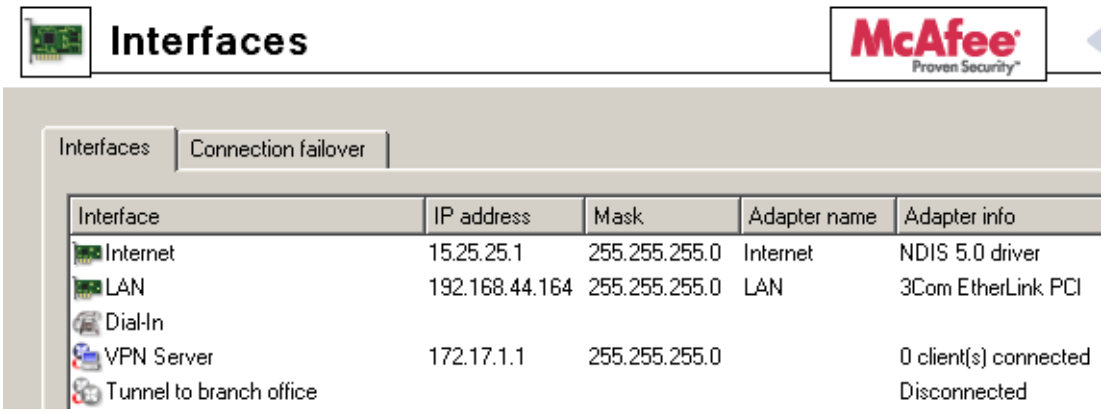


Figure 21.1 Viewing VPN server in the table of interfaces

Double-click on the *VPN server* interface (or select the alternative and press *Edit*, or select *Edit* from the context menu) to open a dialog where parameters of the VPN server can be set.

General

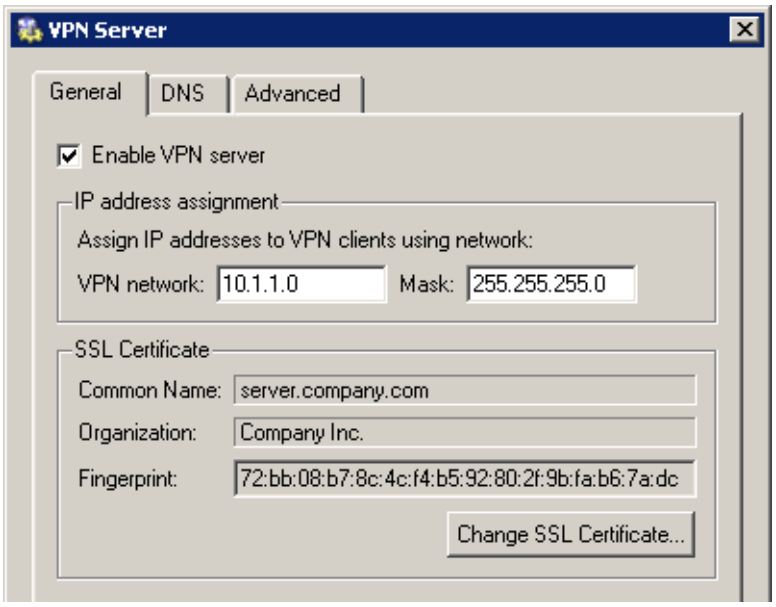


Figure 21.2 VPN server settings — basic parameters

Enable VPN server

Use this option to enable /disable VPN server. VPN server uses TCP and UDP protocols, port 4090 is used as default (the port can be changed in advanced options, however, it is usually not necessary to change it). If the VPN server is not used, it is recommended to disable it.

The action will be applied upon clicking the *Apply* button in the *Interfaces* tab.

IP address assignment

Specification of a subnet (i.e. IP address and a corresponding network mask) from which IP addresses will be assigned to VPN clients and to remote endpoints of VPN tunnels which connect to the server (all clients will be connected through this subnet).

By default (upon the first start-up after installation), *WinRoute* automatically selects a free subnet which will be used for VPN. Under usual circumstances, it is not necessary to change the default subnet. After the first change in VPN server settings, the recently used network is used (the automatic detection is not performed again).

Warning: Make sure that the subnet for VPN clients does not collide with any local subnet!

WinRoute can detect a collision of the VPN subnet with local subnets. The collision may arise when configuration of a local network is changed (change of IP addresses, addition of a new subnet, etc.), or when a subnet for VPN is not selected carefully. If the VPN subnet collides with a local network, a warning message is displayed

upon saving of the settings (by clicking *Apply* in the *Interfaces* tab). In such cases, redefine the VPN subnet.

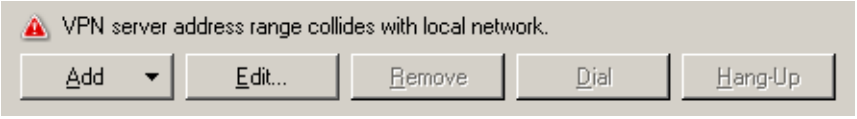


Figure 21.3 VPN server — detection of IP collision

It is recommended to check whether IP collision is not reported after each change in configuration of the local network or/and of the VPN!

Notes:

1. Under certain circumstances, collision with the local network might also arise when a VPN subnet is set automatically (if configuration of the local network is changed later).
2. Regarding two VPN tunnels, it is also examined when establishing a connection whether the VPN subnet does not collide with IP ranges at the other end of the tunnel (remote endpoint).
   If a collision with an IP range is reported upon startup of the VPN server (upon clicking *Apply* in the *Interfaces* tab), the VPN subnet must be set by hand. Select a network which is not used by any of the local networks participating in the connection. VPN subnets at each end of the tunnel must not be identical (two free subnets must be selected).
3. VPN clients can also be assigned IP addresses according to login usernames. For details, see chapter 13.1.

SSL certificate

Information about the current VPN server certificate. This certificate is used for verification of the server's identity during creation of a VPN tunnel (for details, refer to chapter 21.3). The VPN server in *WinRoute* uses the standard SSL certificate.

When defining a VPN tunnel, it is necessary to send the local endpoint's certificate fingerprint to the remote endpoint and vice versa (mutual verification of identity — see chapter 21.3).

HINT: Certificate fingerprint can be saved to the clipboard and pasted to a text file, email message, etc.

Click *Change SSL Certificate* to set parameters for the certificate of the VPN server. For the VPN server, you can either create a custom (self-subscribed) certificate or import a certificate created by a certification authority. The certificate created is saved in the `sslcert` subdirectory of the *WinRoute's* installation directory as `vpn.crt` and the particular private key is saved at the same location as `vpn.key`.

Methods used for creation and import of SSL certificates are described thoroughly in chapter 9.1.

Note: If you already have a certificate created by a certification authority especially for your server (e.g. for secured Web interface), it is also possible to use it for the

VPN server — it is not necessary to apply for a new certificate.

DNS

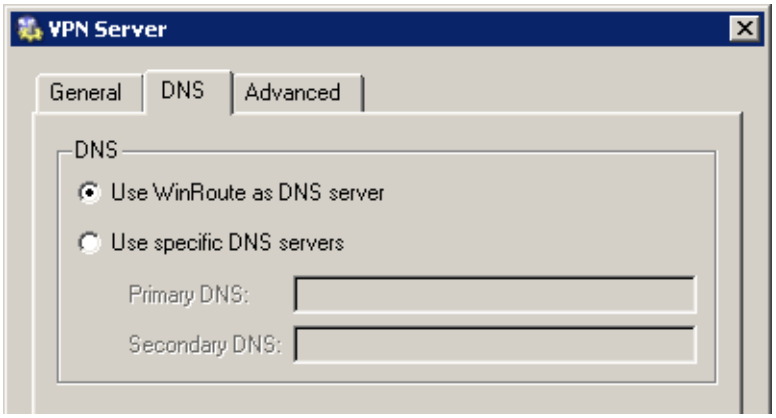


Figure 21.4 VPN server settings — specification of DNS servers

Specify a DNS server which will be used for VPN clients:

- *Use WinRoute as DNS server* — IP address of a corresponding interface of *WinRoute* host will be used as a DNS server for VPN clients (VPN clients will use the *DNS forwarder*).

  If the *DNS Forwarder* is already used as a DNS server for local hosts, it is recommended to use it also for VPN clients. The *DNS forwarder* provides the fastest responses to client DNS requests and possible collision (inconsistency) of DNS records will be avoided.

  Note: If the *DNS forwarder* is disabled (refer to chapter 5.3), the option is not available.

- *Use specific DNS servers* — primary and secondary DNS servers specified through this option will be set for VPN clients.

  If another DNS server than the *DNS forwarder* in *WinRoute* is used in the local network, use this option.

Advanced

Listen on port

The port on which the VPN server listens for incoming connections (both TCP and UDP protocols are used). The port 4090 is set as default (under usual circumstances it is not necessary to switch to another port).

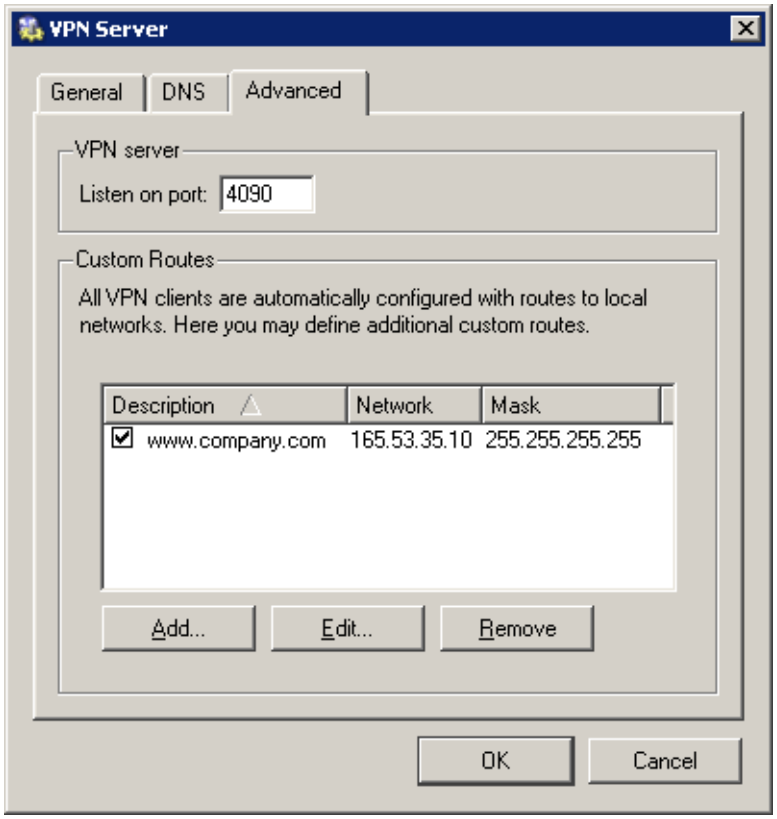


Figure 21.5 VPN server settings — server port and routes for VPN clients

Notes:

1. If the VPN server is already running, all VPN clients will be automatically disconnected during the port change.
2. If it is not possible to run the VPN server at the specified port (the port is used by another service), the following error will be reported in the *Error* log (see chapter 20.8) upon clicking on the *Apply* button:

   ```
   (4103:10048) Socket error: Unable to bind socket
     for service to port 4090.
   (5002) Failed to start service "VPN"
     bound to address 192.168.1.1.
   ```

   To make sure that the specified port is really free, view the *Error* log to see whether an error of this type has not been reported.

Custom Routes

Other networks to which a VPN route will be set for the client can be specified in this section. By default, routes to all local subnets at the VPN server's side are defined — see chapter 21.4).

HINT: Use the `255.255.255.255` network mask to define a route to a certain host. This can be helpful for example when a route to a host in the demilitarized zone at the VPN server's side is being added.

21.2 Configuration of VPN clients

The following conditions must be met to enable connection of remote clients to local networks via encrypted channels:

- The *Kerio VPN Client* must be installed at remote clients (for detailed description, refer to a stand-alone document, *Kerio VPN Client — User Guide*).
- Users whose accounts are used for authentication to *Kerio VPN Client* must possess rights enabling them connect to the VPN server in *WinRoute* (see chapter 13.113.1).
- Connection to the VPN server from the Internet as well as communication between VPN clients must be allowed by traffic rules.

Note: Remote VPN clients connecting to*WinRoute* are included toward the number of persons using the license (see chapters 4 and 4.6). Be aware of this fact when deciding what license type should be bought (or whether an upgrade to a higher number of users should be bought).

Basic configuration of traffic rules for VPN clients

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN Firewall VPN clients	LAN Firewall VPN clients	Any	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.6 Common traffic rules for VPN clients

- The first rule allows communication between the firewall, local network and VPN clients.
- The second rule allows connection to the VPN server in *WinRoute* from the Internet.

  To restrict the number of IP addresses from which connection to the VPN server will be allowed, edit the *Source* entry.

  By default, the *Kerio VPN* service is defined for TCP and UDP protocols, port 4090. If the VPN server is running at another port, this service must be redefined.

If the rules are set like this, all VPN clients can access local networks and vice versa (all local hosts can communicate with all VPN clients). To restrict the type of network access available to VPN clients, special rules must be defined. A few alternatives of the restrictions settings within *Kerio VPN* are focused in chapter 21.5.

Notes:

1. If the *Network Rules Wizard* is used to create traffic rules, the described rules can be generated automatically (including matching of VPN clients with the *Source* and *Destination* items). To generate the rules automatically, select *Yes, I want to use Kerio VPN* in Step 5. For details, see chapter 6.1.

2. For access to the Internet, VPN clients use their current Internet connections. VPN clients are not allowed to connect to the Internet via *WinRoute* (configuration of default gateway of clients cannot be defined).

3. For detailed information about traffic rules, refer to chapter 6.

21.3 Interconnection of two private networks via the Internet (VPN tunnel)

WinRoute (version *6.0.0* or later) including support for VPN (VPN support is included in the typical installation — see chapter 2.3) must be installed in both networks to enable creation of an encrypted tunnel between a local and a remote network via the Internet ("VPN tunnel").

Note: Each installation of *WinRoute* requires its own license (see chapter 4).

Setting up VPN servers

First, the VPN server must be allowed by the traffic policy and enabled at both ends of the tunnel. For detailed description on configuration of VPN servers, refer to chapter 21.1.

Definition of a tunnel to a remote server

VPN tunnel to the server on the other side must be defined at both ends. Use the *Add* → *VPN tunnel* option in the *Interfaces* section to create a new tunnel.

Name of the tunnel

Each VPN tunnel must have a unique name. This name will be used in the table of interfaces, in traffic rules (see chapter 6.3) and interface statistics (details in chapter 18.1).

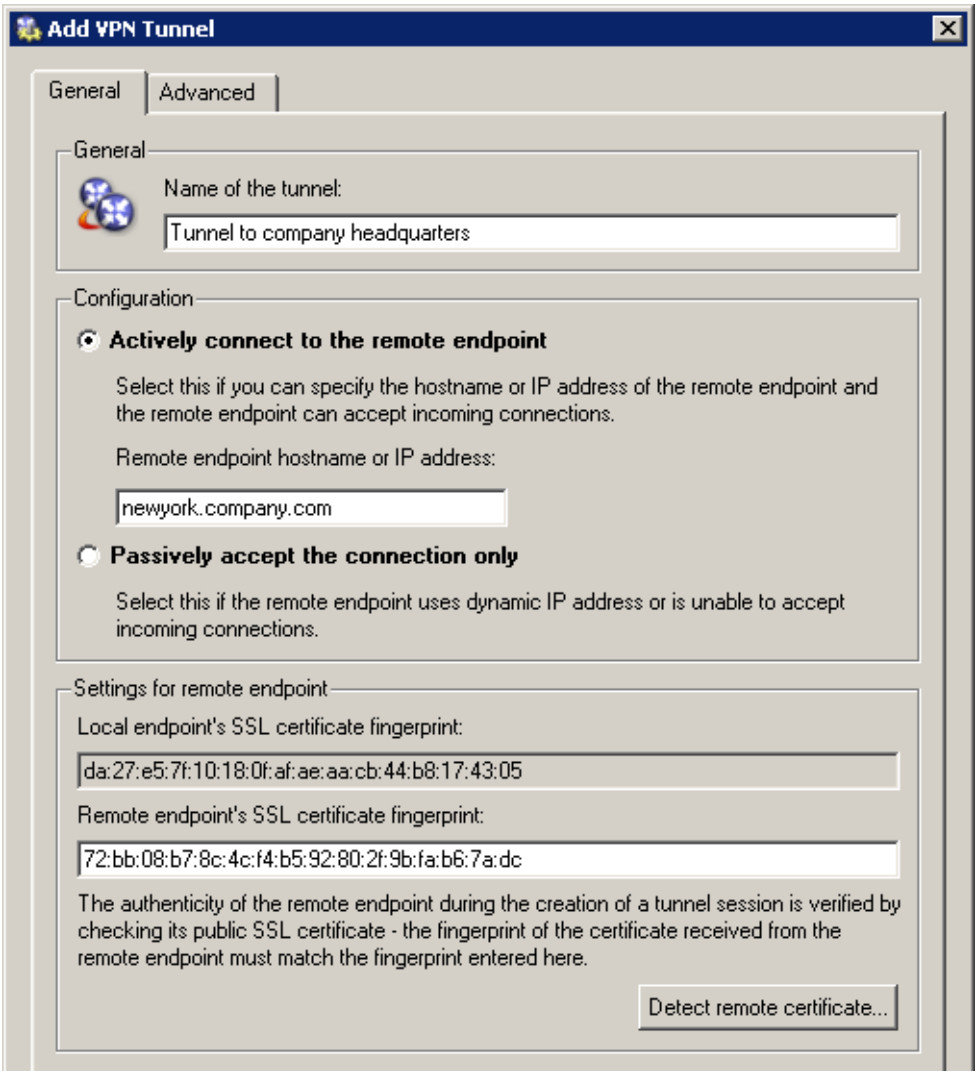

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to company headquarters
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
newyork.company.com
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
Remote endpoint's SSL certificate fingerprint:
72:bb:08:b7:8c:4c:f4:b5:92:80:2f:9b:fa:b6:7a:dc
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.7 VPN tunnel configuration

Configuration

Selection of a mode for the local end of the tunnel:

- *Active* — this side of the tunnel will automatically attempt to establish and maintain a connection to the remote VPN server.
  The remote VPN server specification is required through the *Remote hostname or IP address* entry. If the remote VPN server does not use the port 4090, a corresponding port number separated by a colon must be specified (e.g. `server.company.com:4100` or `10.10.100.20:9000`).
  This mode is available if the IP address or DNS name of the other side of the tunnel is known and the remote endpoint is allowed to accept incoming connections (i.e. the communication is not blocked by a firewall at the remote end of

the tunnel).

- *Passive* — this end of the tunnel will only listen for an incoming connection from the remote (active) side.
  The passive mode is only useful when the local end of the tunnel has a fixed IP address and when it is allowed to accept incoming connections.

At least one end of each VPN tunnel must be switched to the active mode (passive servers cannot initialize connection).

Configuration of a remote end of the tunnel

When a VPN tunnel is being created, identity of the remote endpoint is authenticated through the fingerprint of its SSL certificate. If the fingerprint does not match with the fingerprint specified in the configuration of the tunnel, the connection will be rejected.

The fingerprint of the local certificate and the entry for specification of the remote fingerprint are provided in the *Settings for remote endpoint* section. Specify the fingerprint for the remote VPN server certificate and vice versa — specify the fingerprint of the local server in the configuration at the remote server.

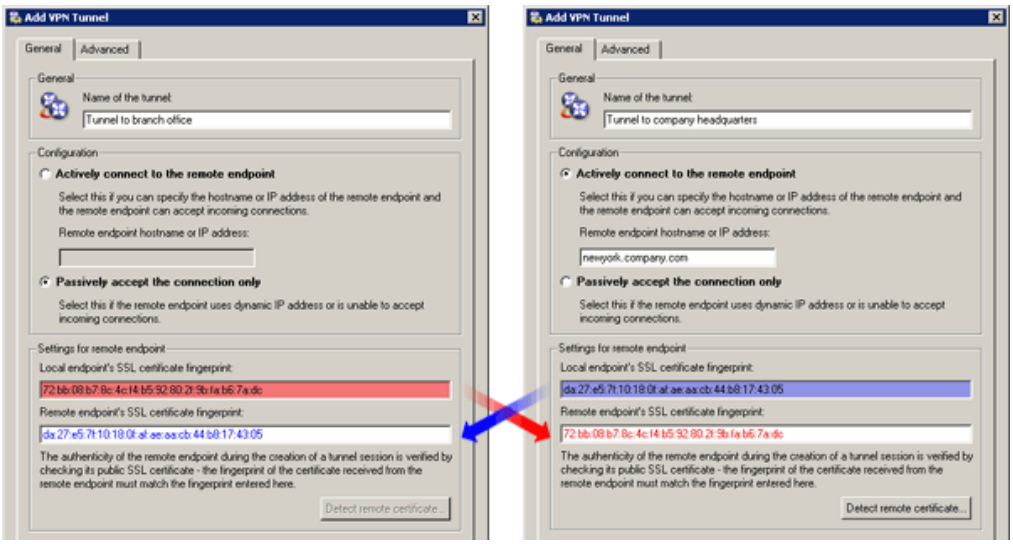


Figure 21.8 VPN tunnel — certificate fingerprints

If the local endpoint is set to the active mode, the certificate of the remote endpoint and its fingerprint can be downloaded by clicking *Detect remote certificate*. Passive endpoint cannot detect remote certificate.

However, this method of fingerprint setting is quite insecure —a counterfeit certificate might be used. If a fingerprint of a false certificate is used for the configuration of the VPN tunnel, it is possible to create a tunnel for the false endpoint (for the attacker). Moreover, a valid certificate would not be accepted from the other side. Therefore, for security reasons, it is recommended to set fingerprints manually.

DNS Settings

DNS must be set properly at both sends of the tunnel so that it is possible to connect to hosts in the remote network using their DNS names. One method is to add DNS records of the hosts (to the hosts file) at each endpoint. However, this method is quite complicated and inflexible.

If the *DNS forwarder* in *WinRoute* is used as the DNS server at both ends of the tunnel, DNS queries (for DNS rules, refer to chapter 5.3) can be forwarded to hostnames in the corresponding domain of the *DNS forwarder* at the other end of the tunnel. DNS domain (or subdomain) must be used at both sides of the tunnel.

Note: To provide correct forwarding of DNS queries sent from the *WinRoute* host (at any side of the VPN tunnel), it is necessary that these queries are processed by *DNS forwarder*. To secure this, set local IP address as for the DNS server and specify former DNS servers in the *WinRoute's DNS forwarder*.

Detailed guidance for the DNS configuration is provided in chapter 21.5.

Routing settings

On the *Advanced* tab, you can set which method will be used to add routes provided by the remote endpoint of the tunnel to the local routing table as well as define custom routes to remote networks.

The *Kerio VPN* routing issue is described in detail in chapter 21.4.

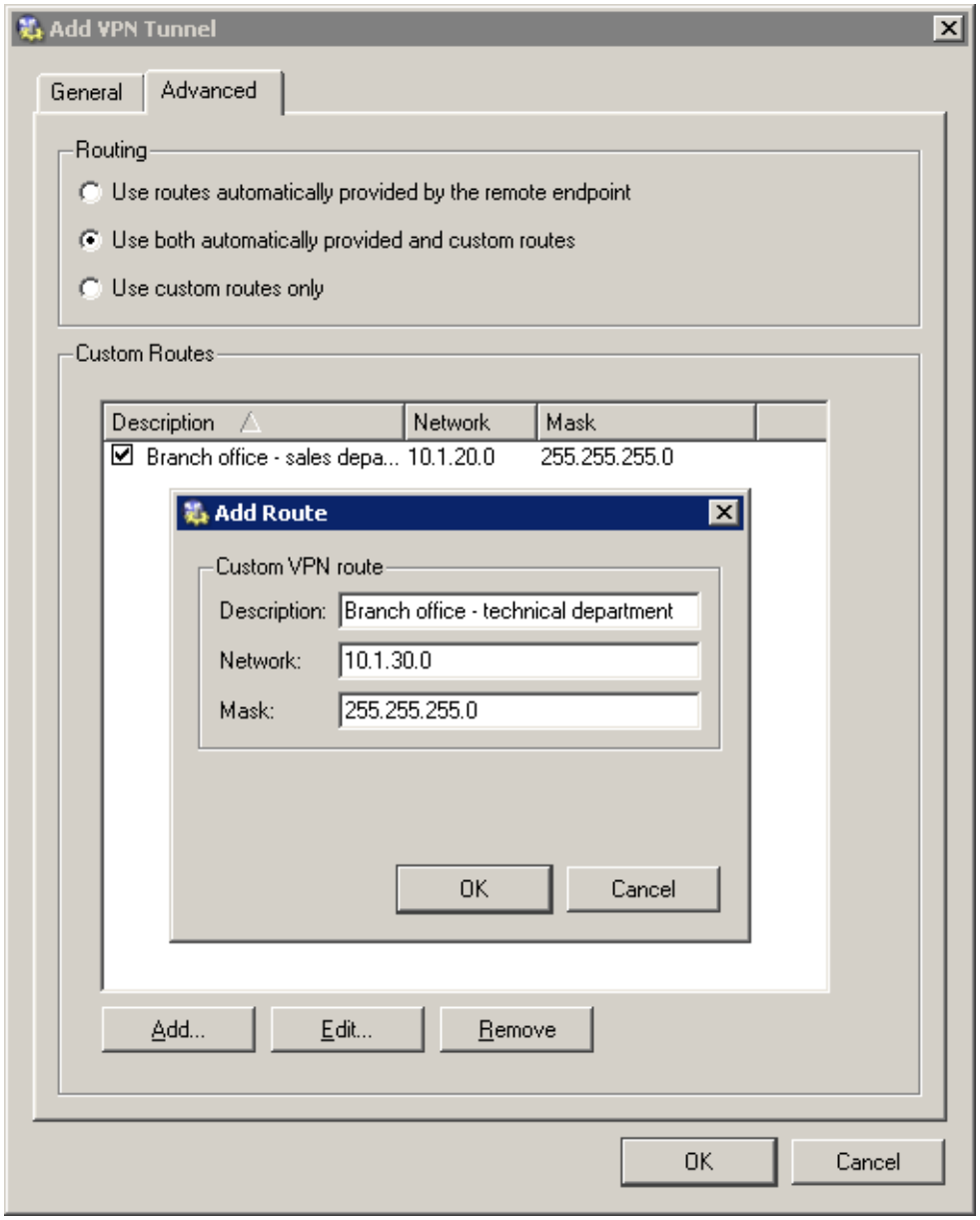


Figure 21.9 VPN tunnel's routing configuration

Connection establishment

Active endpoints automatically attempt to recover connection whenever they detect that the corresponding tunnel has been disconnected (the first connection establishment is attempted immediately after the tunnel is defined and upon clicking the *Apply* button in *Configuration* → *Interfaces*, i.e. when the corresponding traffic is allowed — see below).

VPN tunnels can be disabled by the *Disable* button. Both endpoints should be disabled while the tunnel is being disabled.

Note: VPN tunnels keeps their connection (by sending special packets in regular time intervals) even if no data is transmitted. This feature protects tunnels from disconnection by other firewalls or network devices between ends of tunnels.

Traffic Policy Settings for VPN

Once the VPN tunnel is created, it is necessary to allow traffic between the LAN and the network connected by the tunnel and to allow outgoing connection for the *Kerio VPN* service (from the firewall to the Internet). If basic traffic rules are already created by the wizard (refer to chapter 21.2), simply add a corresponding VPN tunnel into the *Local Traffic* rule and the *Kerio VPN* service to the *Firewall traffic*. The resulting traffic rules are shown at figure 21.10.

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN Firewall VPN clients Tunnel to branch office	LAN Firewall VPN clients Tunnel to branch office	Any	✓	
Firewall Traffic	Firewall	Internet	DNS HTTP HTTPS IMAP Kerio VPN POP3 SMTP Telnet	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.10 Traffic Policy Settings for VPN

Notes:

1. To keep examples in this guide as simple as possible, it is supposed that the *Firewall traffic* rule allows to access any service at the firewall (see figure 21.11). Under these conditions, it is not necessary to add the *Kerio VPN* service to the rule.

2. Traffic rules set by this method allow full IP communication between the local network, remote network and all VPN clients. For access restrictions, define corresponding traffic rules (for local traffic, VPN clients, VPN tunnel, etc.). Examples of traffic rules are provided in chapter 21.5.

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN Firewall VPN clients Tunnel to branch office	LAN Firewall VPN clients Tunnel to branch office	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.11 Common traffic rules for VPN tunnel

21.4 Exchange of routing information

An automatic exchange of routing information (i.e. of data informing about routes to local subnets) is performed between endpoints of any VPN tunnel (or between the VPN server and a VPN client). thus, routing tables at both sides of the tunnel are still kept updated.

Routing configuration options

Under usual circumstances, it is not necessary to define any custom routes — particular routes will be added to the routing tables automatically when configuration is changed at any side of the tunnel (or at the VPN server). However, if a routing table at any side of the VPN tunnel includes invalid routes (e.g. specified by the administrator), these routes are also interchanged. This might make traffic with some remote subnets impossible and overload VPN tunnel by too many control messages.

A similar problem may occur in case of a VPN client connecting to the *WinRoute's* VPN server.

To avoid the problems just described, it is possible to go to the VPN tunnel definition dialog (see chapter 21.3) or to the VPN server settings dialog (refer to chapter 21.1) to set which routing data will be used and define custom routes.

Kerio VPN uses the following methods to pass routing information:

- *Routes provided automatically by the remote endpoint* (set as default) — routes to remote networks are set automatically with respect to the information provided by the remote endpoint. If this option is selected, no additional settings are necessary unless problems regarding invalid routes occur (see above).

- *Both automatically provided and custom routes* — routes provided automatically are complemented by custom routes defined at the local endpoint. In case of any colli-

sions, custom routes are used as prior. This option easily solves the problem where a remote endpoint provides one or more invalid route(s).

- *Custom routes only* — all routes to remote networks must be set manually at the local endpoint of the tunnel. This alternative eliminates adding of invalid routes provided by a remote endpoint to the local routing table. However, it is quite demanding from the administrator's point of view (any change in the remote network's configuration requires modification of custom routes).

Routes provided automatically

Unless any custom routes are defined, the following rules apply to the interchange of routing information:

- default routes as well as routes to networks with default gateways are not exchanged (default gateway cannot be changed for remote VPN clients and/or for remote endpoints of a tunnel),
- routes to subnets which are identical for both sides of a tunnel are not exchanged (routing of local and remote networks with identical IP ranges is not allowed).
- other routes (i.e. routes to local subnets at remote ends of VPN tunnels excluding the cases described above, all other VPN and all VPN clients) are exchanged.

Note: As implied from the description provided above, if two VPN tunnels are created, communication between these two networks is possible. The traffic rules can be configured so that connection to the local network will be disabled for both these remote networks.

Update of routing tables

Routing information is exchanged:

- when a VPN tunnel is connected or when a VPN client is connected to the server,
- when information in a routing table at any side of the tunnel (or at the VPN server) is changed,
- periodically, once per 30 secs (VPN tunnel) or once per 1 min (VPN client). The timeout starts upon each update (regardless of the update reason).

21.5 Example of Kerio VPN configuration: company with a filial office

This chapter provides a detailed exemplary description on how to create an encrypted tunnel connecting two private networks using the *Kerio VPN*.

This example can be easily customized. The method described can be used in cases where no redundant routes arise by creating VPN tunnels (i.e. multiple routes between individual private networks). Configuration of VPN with redundant routes (typically in case of a company with two or more filials) is described in chapter 21.6.

Note: This example describes a more complicated pattern of VPN with access restrictions for individual local networks and VPN clients. An example of basic VPN configuration is provided in the *Kerio WinRoute Firewall — Step By Step Configuration* document.

Specification

Supposing a company has its headquarters in New York and a branch office in London. We intend to interconnect local networks of the headquarters by a VPN tunnel using the *Kerio VPN*. VPN clients will be allowed to connect to the headquarters network.

The server (default gateway) of the headquarters uses the public IP address `63.55.21.12` (DNS name is `newyork.company.com`), the server of the branch office uses a dynamic IP address assigned by DHCP.

The local network of the headquarters consists of two subnets, `LAN 1` and `LAN 2`. The headquarters uses the `company.com` DNS domain.

The network of the branch office consists of one subnet only (`LAN`). The branch office `filial.company.com`.

Figure 21.12 provides a scheme of the entire system, including IP addresses and the VPN tunnels that will be built.

Suppose that both networks are already deployed and set according to the figure and that the Internet connection is available.

Traffic between the network of the headquarters, the network of the branch office and VPN clients will be restricted according to the following rules:

1. VPN clients can connect to the `LAN 1` and to the network of the branch office.
2. Connection to VPN clients is disabled for all networks.
3. Only the `LAN 1` network is available from the branch office. In addition to this, only the *WWW*, *FTP* and *Microsoft SQL* services are available.

4. No restrictions are applied for connections from the headquarters to the branch office network.

5. LAN 2 is not available to the branch office network nor to VPN clients.

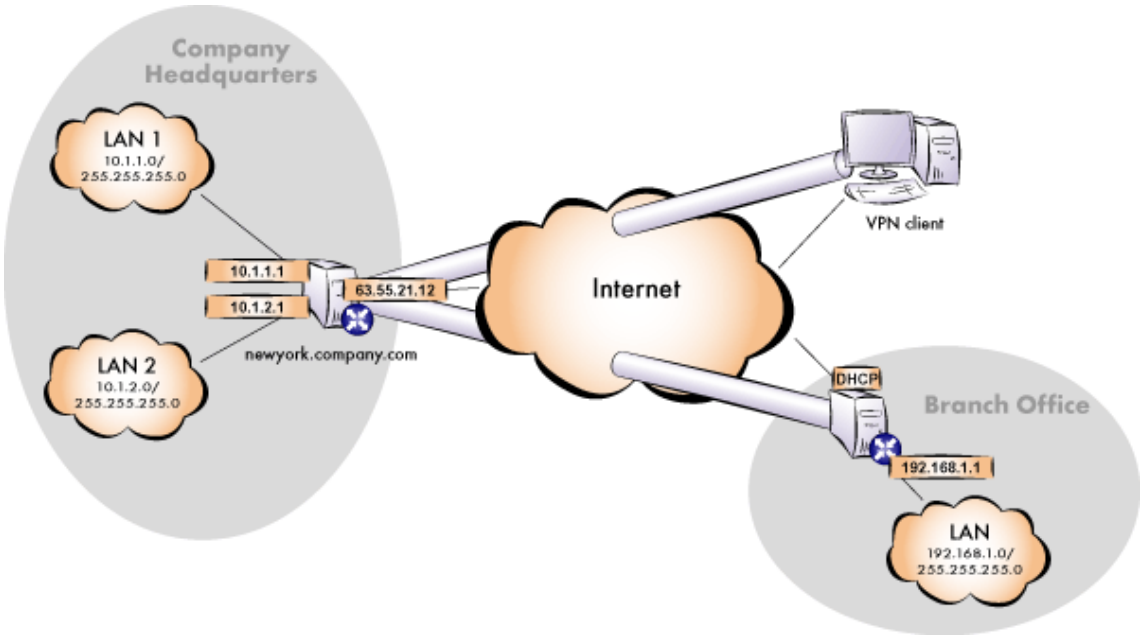


Figure 21.12 Example — interconnection of the headquarter and a filial office by VPN tunnel (connection of VPN clients is possible)

Common method

The following actions must be taken in both local networks (i.e. in the main office and the filial):

1. It is necessary that *WinRoute* in version 6.0.0 or higher (older versions do not include *Kerio VPN*) is installed at the default gateway.

   Note: For *each* installation of *WinRoute*, a separate license for corresponding number of users is required! For details see chapter 4.

2. Configure and test connection of the local network to the Internet. Hosts in the local network must use the *WinRoute* host's IP address as the default gateway and as the primary DNS server.

   If it is a new (clean) *WinRoute* installation, it is possible to use the traffic rule wizard (refer to chapter 6.1).

For detailed description of basic configuration of *WinRoute* and of the local network, refer to the *Kerio WinRoute Firewall — Step By Step* document.

3. In configuration of *DNS Forwarder*, set DNS forwarding rules for the domain in the remote network. This enables to access hosts in the remote network by using their DNS names (otherwise, it is necessary to specify remote hosts by IP addresses).

   To provide correct forwarding of DNS requests from a *WinRoute* host, it is necessary to use an IP address of a network device belonging to the host as the primary DNS server. In *DNS Forwarder* configuration, at least one DNS server must be specified to which DNS queries for other domains (typically the DNS server of the ISP).

   Note: For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the `hosts` file (if they use IP addresses) or enable co-operation of the *DNS Forwarder* with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 5.3.

4. In the *Interfaces* section, allow the VPN server and set its SSL certificate if necessary. Note the fingerprint of the server's certificate for later use (it will be required for configuration of the remote endpoint of the VPN tunnel).

   Check whether the automatically selected VPN subnet does not collide with any local subnet either in the headquarters or in the filial and select another free subnet if necessary.

5. Define the VPN tunnel to the remote network. The passive endpoint of the tunnel must be created at a server with fixed public IP address (i.e. at the headquarter's server). Only active endpoints of VPN tunnels can be created at servers with dynamic IP address.

   If the remote endpoint of the tunnel has already been defined, check whether the tunnel was created. If not, refer to the *Error* log, check fingerprints of the certificates and also availability of the remote server.

6. In traffic rules, allow traffic between the local network, remote network and VPN clients and set desirable access restrictions. In this network configuration, all desirable restrictions can be set at the headquarter's server. Therefore, only traffic between the local network and the VPN tunnel will be enabled at the filial's server.

7. Test reachability of remote hosts from each local network. To perform the test, use the `ping` and `tracert` system commands. Test availability of remote hosts both through IP addresses and DNS names.

If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

If an IP address is tested successfully and an error is reported (*Unknown host*) when a corresponding DNS name is tested, then check configuration of the DNS.

The following sections provide detailed description of the *Kerio VPN* configuration both for the headquarter and the filial offices.

Headquarters configuration

1. Install *WinRoute* (version `6.0.0` or later) at the headquarter's default gateway ("server").

2. Use *Network Rules Wizard* (see chapter 6.1) to configure the basic traffic policy in *WinRoute*. To keep the example as simple as possible, it is supposed that the access from the local network to the Internet is not restricted, i.e. that access to all services is allowed in step 4.

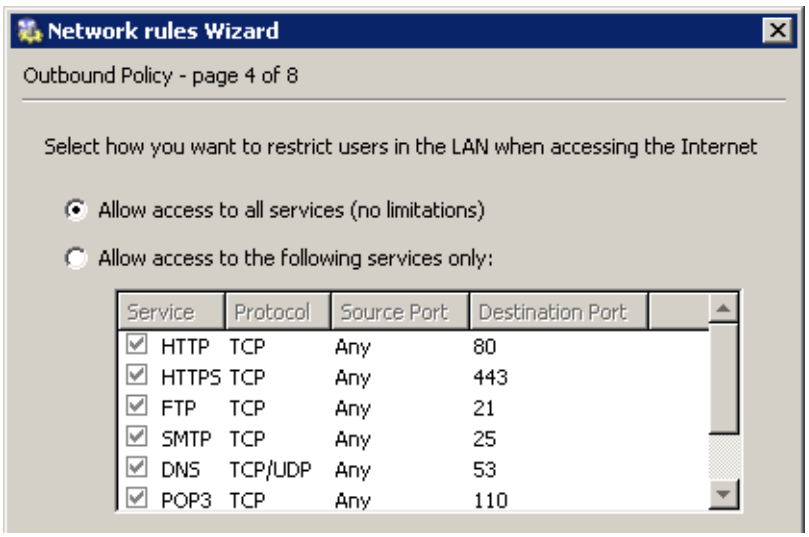

Network rules Wizard
Outbound Policy - page 4 of 8
Select how you want to restrict users in the LAN when accessing the Internet
Allow access to all services (no limitations)
Allow access to the following services only:
Service
Protocol
Source Port
Destination Port
HTTP TCP Any 80
HTTPS TCP Any 443
FTP TCP Any 21
SMTP TCP Any 25
DNS TCP/UDP Any 53
POP3 TCP Any 110

Figure 21.13 Headquarters — no restrictions are applied to accessing the Internet from the LAN

In step 5, select *Create rules for Kerio VPN server*. Status of the *Create rules for Kerio Clientless SSL-VPN* option is irrelevant (this example does not include *Clientless SSL-VPN* interface's issues).

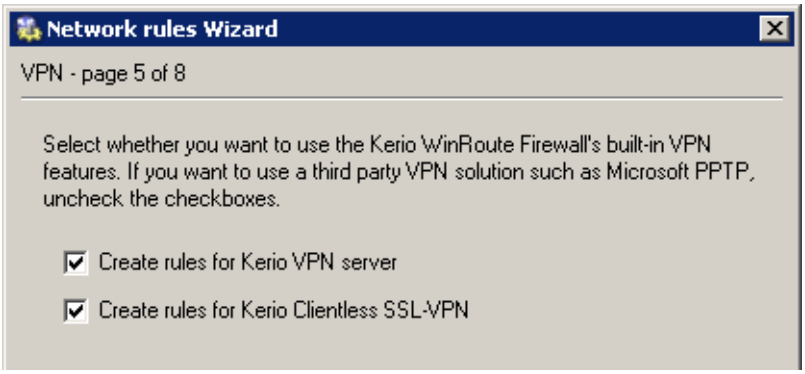

Network rules Wizard
VPN - page 5 of 8
Select whether you want to use the Kerio WinRoute Firewall's built-in VPN features. If you want to use a third party VPN solution such as Microsoft PPTP, uncheck the checkboxes.
Create rules for Kerio VPN server
Create rules for Kerio Clientless SSL-VPN

Figure 21.14 Headquarter — creating default traffic rules for Kerio VPN

This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

Name	Source	Destination	Service	Action	Translation
Local Traffic	Dial-In LAN 1 LAN 2 Firewall VPN clients	Dial-In LAN 1 LAN 2 Firewall VPN clients	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.15 Headquarter — default traffic rules for Kerio VPN

When the VPN tunnel is created, customize these rules according to the restriction requirements (see item 6).

Note: To keep the example as simple and transparent as possible, only traffic rules relevant for the *Kerio VPN* configuration are mentioned.

3. Customize DNS configuration as follows:

   - In configuration of the *DNS Forwarder* in *WinRoute*, specify DNS servers to which DNS queries which are not addressed to the `company.com` domain will be forwarded (primary and secondary DNS server of the Internet connection provider by default).

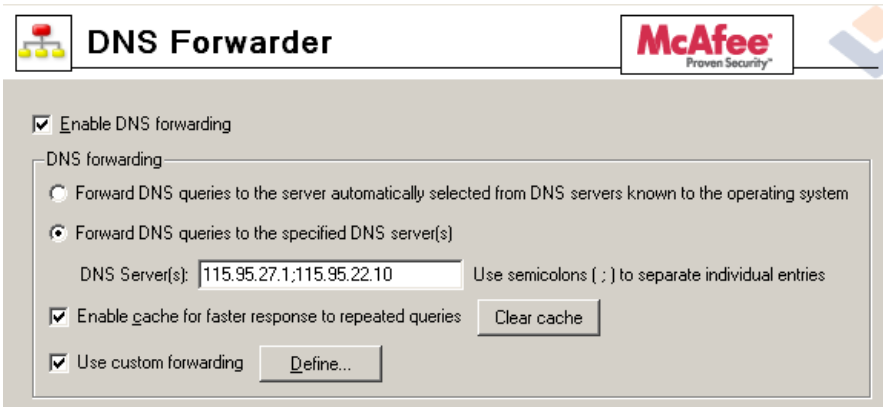

DNS Forwarder
McAfee
Proven Security
Enable DNS forwarding
DNS forwarding
Forward DNS queries to the server automatically selected from DNS servers known to the operating system
Forward DNS queries to the specified DNS server(s)
DNS Server(s):
115.95.27.1;115.95.22.10
Use semicolons (;) to separate individual entries
Enable cache for faster response to repeated queries
Clear cache
Use custom forwarding
Define...

Figure 21.16 Headquarter — DNS forwarder configuration

- Enable the *Use custom forwarding* option and define rules for names in the `filial.company.com` domain. Specify the server for DNS forwarding by the IP address of the remote firewall host's interface (i.e. interface connected to the local network at the other end of the tunnel).

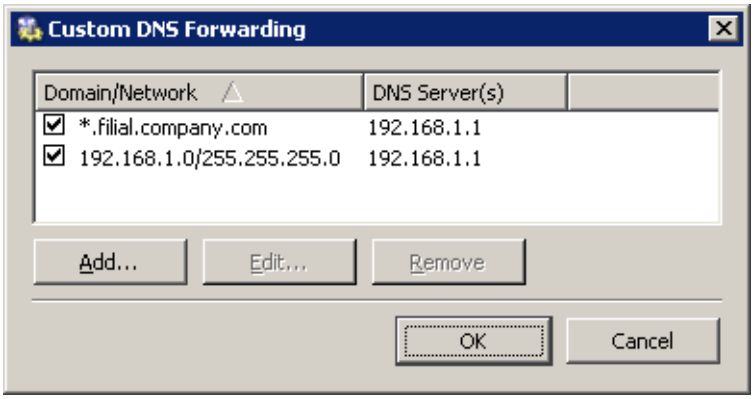


Figure 21.17 Headquarter — DNS forwarding settings

- Set the IP address of this interface (`10.1.1.1`) as a primary DNS server for the *WinRoute* host's interface connected to the *LAN 1* local network. It is not necessary to set DNS server at the interface connected to *LAN 2* — DNS configuration is applied globally to the entire operating system.

- Set the IP address `10.1.1.1` as a primary DNS server also for the other hosts.

Note: For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the `hosts` file (if they use IP addresses) or enable cooperation of the *DNS Forwarder* with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 5.3.

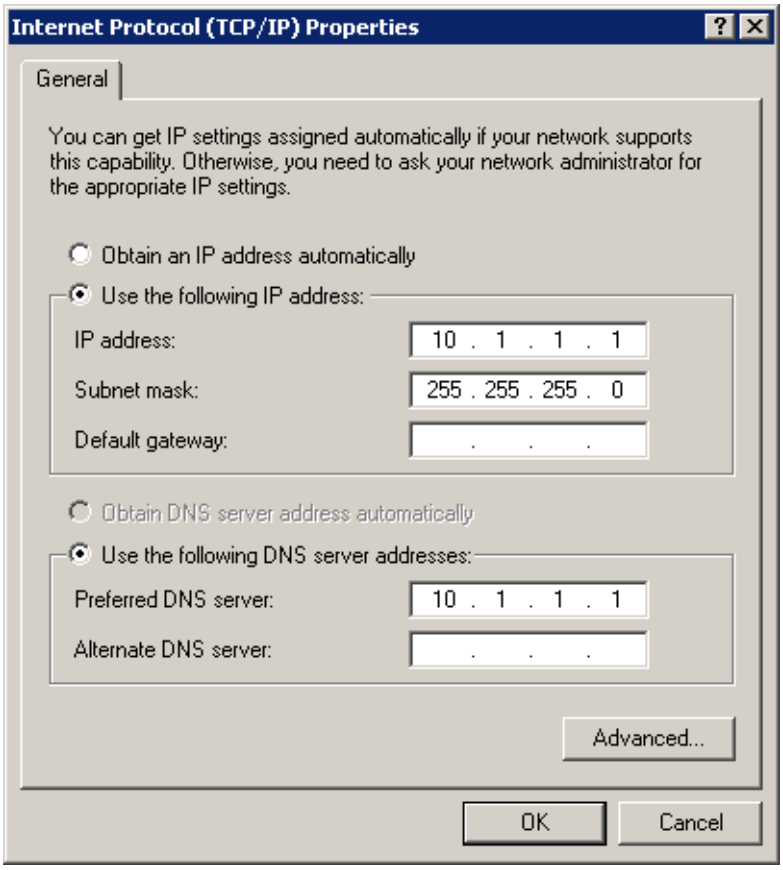

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 1 . 1 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
10 . 1 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Figure 21.18 Headquarter — TCP/IP configuration
at a firewall's interface connected to the local network

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: A free subnet which has been selected is now specified automatically in the *VPN network* and *Mask* entries.

   For a detailed description on the VPN server configuration, refer to chapter 21.1.

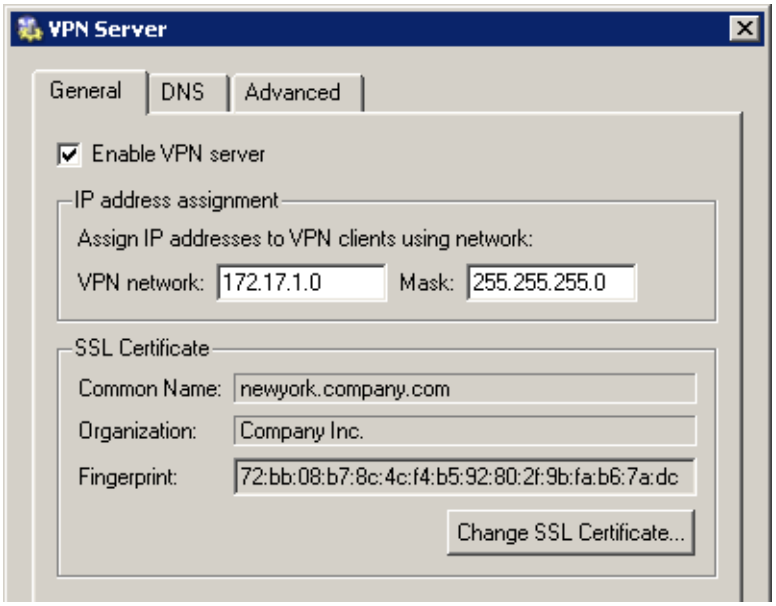


Figure 21.19 Headquarters — VPN server configuration

5. Create a passive end of the VPN tunnel (the server of the branch office uses a dynamic IP address). Specify the remote endpoint's fingerprint by the fingerprint of the certificate of the branch office VPN server.

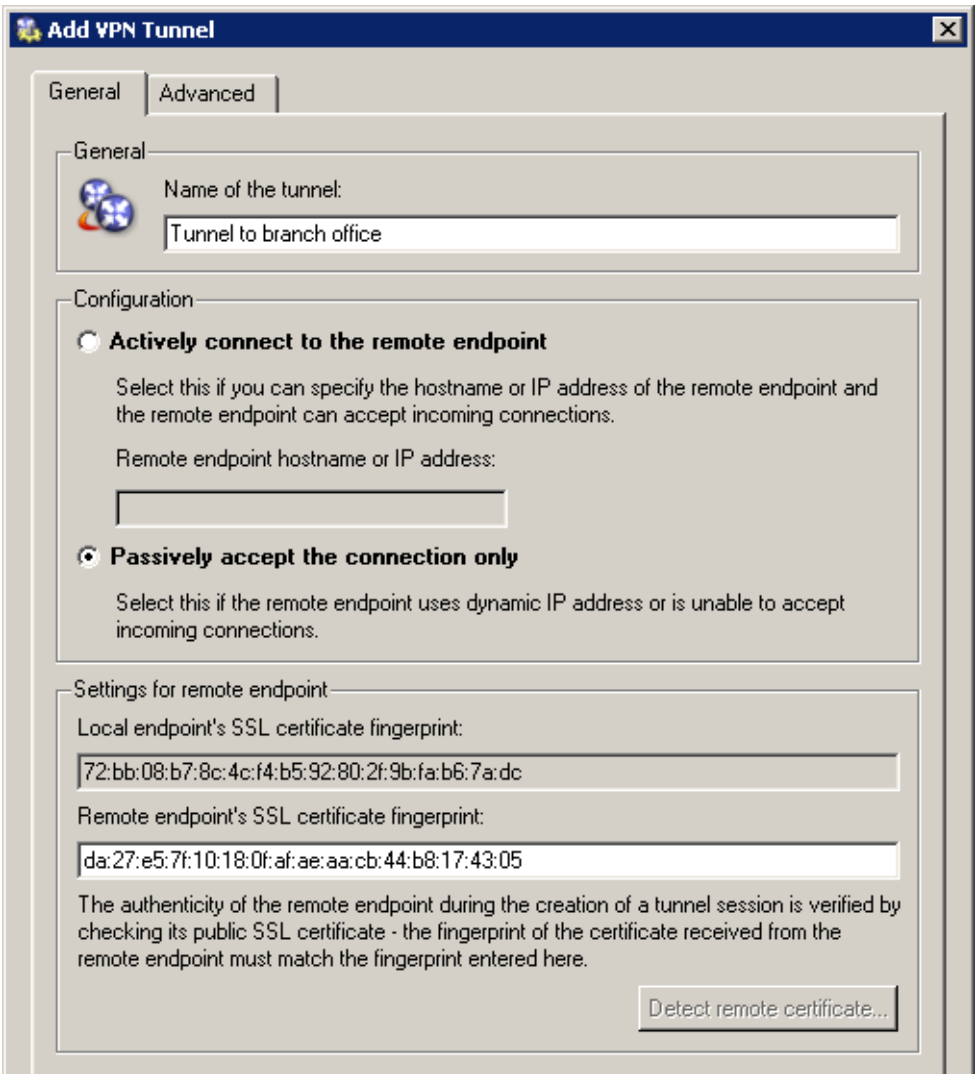

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to branch office
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
72:bb:08:b7:8c:4c:f4:b5:92:80:2f:9b:fa:b6:7a:dc
Remote endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.20 Headquarter — definition of VPN tunnel for a filial office

6. Customize traffic rules according to the restriction requirements.

   - In the *Local Traffic* rule, remove all items except those belonging to the local network of the company headquarters, i.e. except the firewall and `LAN 1` and `LAN 2`.

   - Define (add) the *VPN clients* rule which will allow VPN clients to connect to `LAN 1` and to the network of the branch office (via the VPN tunnel).

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN 1 LAN 2 Firewall	LAN 1 LAN 2 Firewall	Any	✓	
VPN Clients	VPN clients	LAN 1 Tunnel to branch office	Any	✓	
Branch office	Tunnel to branch office	LAN 1	FTP HTTP MS-SQL	✓	
Company headquarters	LAN 1 LAN 2	Tunnel to branch office	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
Service Kerio VPN	Internet	Firewall	Kerio VPN	✓	

Figure 21.21 Headquarter — final traffic rules

- Create the *Branch office* rule which will allow connections to services in `LAN 1`.
- Add the *Company headquarters* rule allowing connections from both headquarters subnets to the branch office network..

Rules defined this way meet all the restriction requirements. Traffic which will not match any of these rules will be blocked by the default rule (see chapter 6.3).

Configuration of a filial office

1. Install *WinRoute* (version `6.0.0` or later) at the default gateway of the branch office ("server").

2. Use *Network Rules Wizard* (see chapter 6.1) to configure the basic traffic policy in *WinRoute*. To keep the example as simple as possible, it is supposed that the access from the local network to the Internet is not restricted, i.e. that access to all services is allowed in step 4.

   In this case, it would be meaningless to create rules for the *Kerio VPN server* and/or the *Kerio Clientless SSL-VPN*, since the server uses a dynamic public IP address). Therefore, leave these options disabled in step 5.

   This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

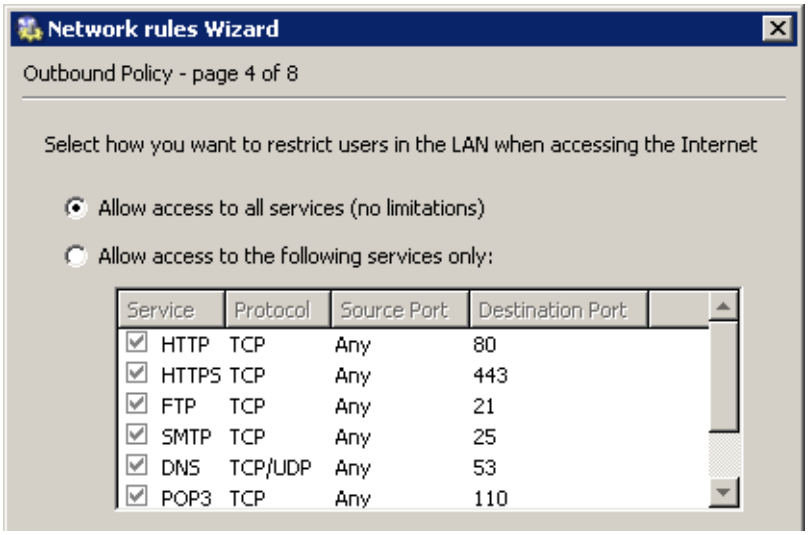

Network rules Wizard
Outbound Policy - page 4 of 8
Select how you want to restrict users in the LAN when accessing the Internet
Allow access to all services (no limitations)
Allow access to the following services only:
Service
Protocol
Source Port
Destination Port
HTTP TCP Any 80
HTTPS TCP Any 443
FTP TCP Any 21
SMTP TCP Any 25
DNS TCP/UDP Any 53
POP3 TCP Any 110

Figure 21.22 Filial — no restrictions are applied to accessing the Internet from the LAN

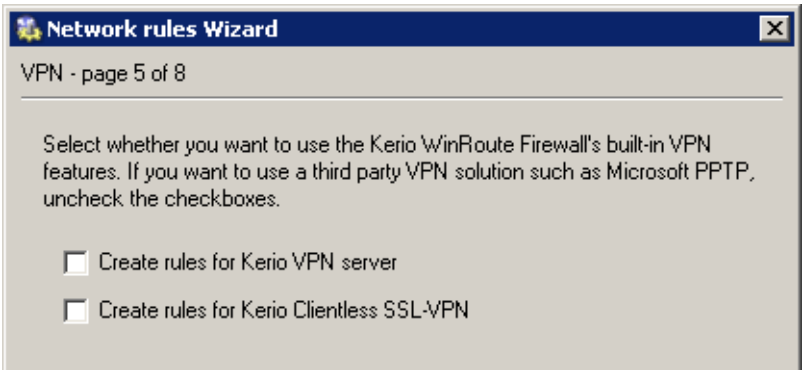

Network rules Wizard
VPN - page 5 of 8
Select whether you want to use the Kerio WinRoute Firewall's built-in VPN features. If you want to use a third party VPN solution such as Microsoft PPTP, uncheck the checkboxes.
Create rules for Kerio VPN server
Create rules for Kerio Clientless SSL-VPN

Figure 21.23 A filial — it is not necessary to create rules for the Kerio VPN server

Name	Source	Destination	Service	Action	Translation
Local Traffic	Dial-In LAN Firewall VPN clients	Dial-In LAN Firewall VPN clients	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.24 Filial office — default traffic rules for Kerio VPN

When the VPN tunnel is created, customize these rules according to the restriction requirements (Step 6).

3. Customize DNS configuration as follows:

   - In configuration of the *DNS Forwarder* in *WinRoute*, specify DNS servers to which DNS queries which are not addressed to the `company.com` domain will be forwarded (primary and secondary DNS server of the Internet connection provider by default).

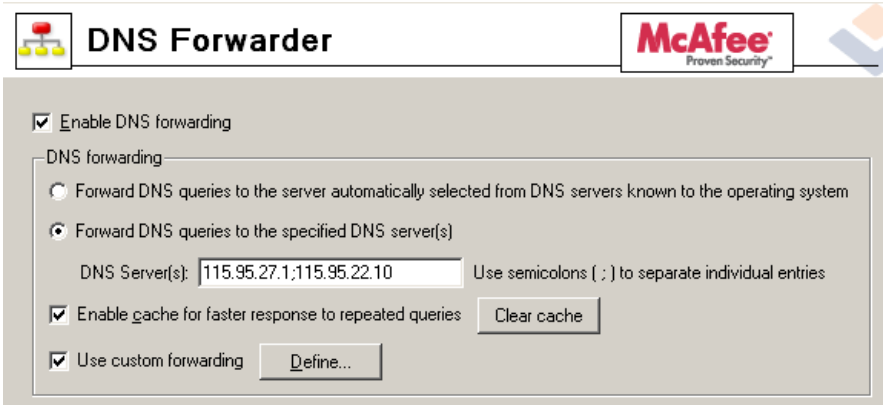

DNS Forwarder
McAfee
Proven Security
Enable DNS forwarding
DNS forwarding
Forward DNS queries to the server automatically selected from DNS servers known to the operating system
Forward DNS queries to the specified DNS server(s)
DNS Server(s):
115.95.27.1;115.95.22.10
Use semicolons (;) to separate individual entries
Enable cache for faster response to repeated queries
Clear cache
Use custom forwarding
Define...

Figure 21.25 Filial office — DNS forwarder configuration

   - Enable the *Use custom forwarding* option and define rules for names in the `filial.company.com` domain. Specify the server for DNS forwarding by the IP address of the remote firewall host's interface (i.e. interface connected to the local network at the other end of the tunnel).

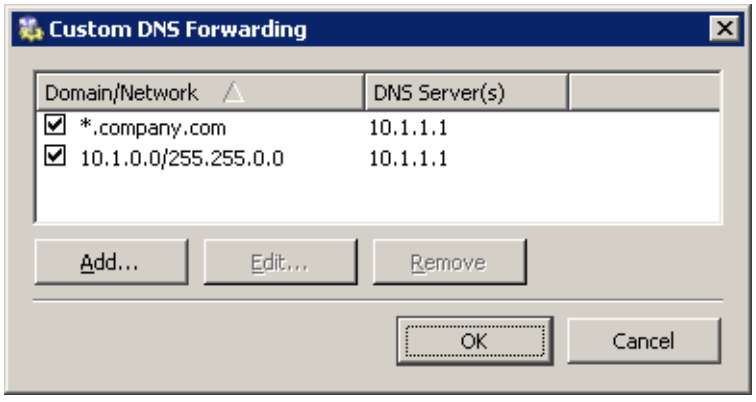


Figure 21.26 Filial office — DNS forwarding settings

- Set the IP address of this interface (`192.168.1.1`) as a primary DNS server for the *WinRoute* host's interface connected to the local network.

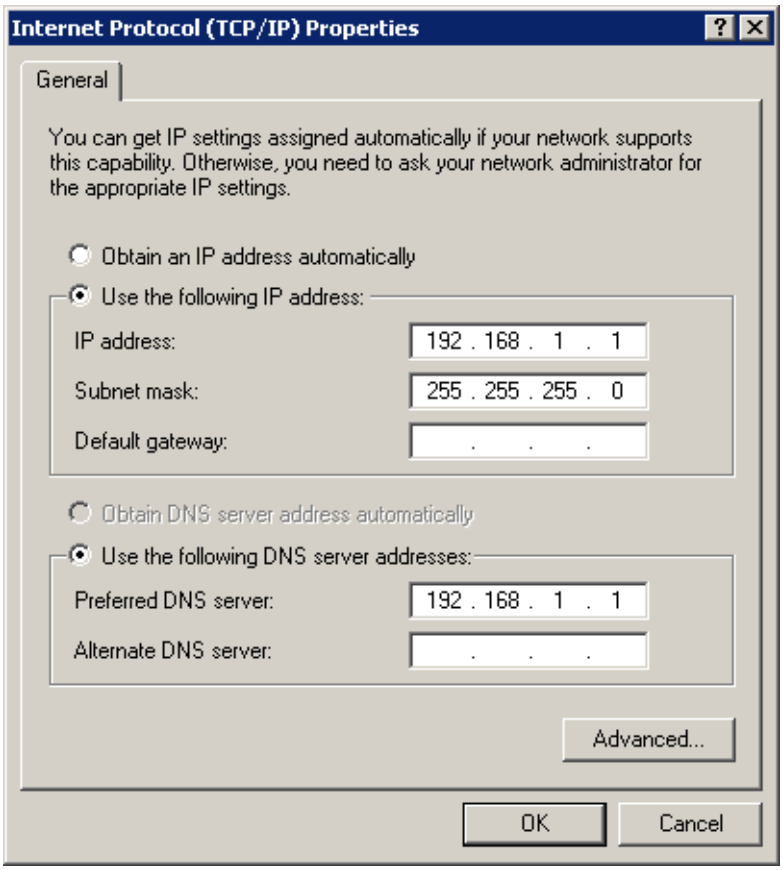

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Figure 21.27 Filial office — TCP/IP configuration at a firewall's interface connected to the local network

- Set the IP address `192.168.1.1` as a primary DNS server also for the other hosts.

Note: For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the `hosts` file (if they use IP addresses) or enable co-operation of the *DNS Forwarder* with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 5.3.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: A free subnet which has been selected is now specified automatically in the *VPN network* and *Mask* entries.

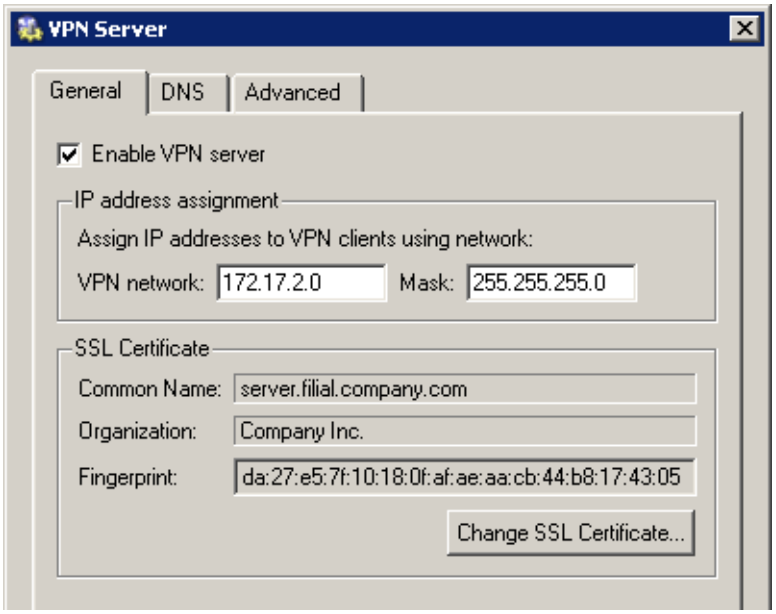


Figure 21.28 Filial office — VPN server configuration

For a detailed description on the VPN server configuration, refer to chapter 21.1.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (`newyork.company.com`). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.

   At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the *Connected* status will be reported in the *Adapter info* column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server — in our example, the `ping newyork.company.com` command can be used at the branch office server.

   Note: If a collision of VPN network and the remote network is detected upon creation of the VPN tunnel, select an appropriate free subnet and specify its parameters at the VPN server (see Step 4).

   For detailed information on how to create VPN tunnels, see chapter 21.3.

6. Add the new VPN tunnel into the *Local Traffic* rule. It is also possible to remove the *Dial-In* interface and the *VPN clients* group from this rule (VPN clients are not allowed to connect to the branch office).

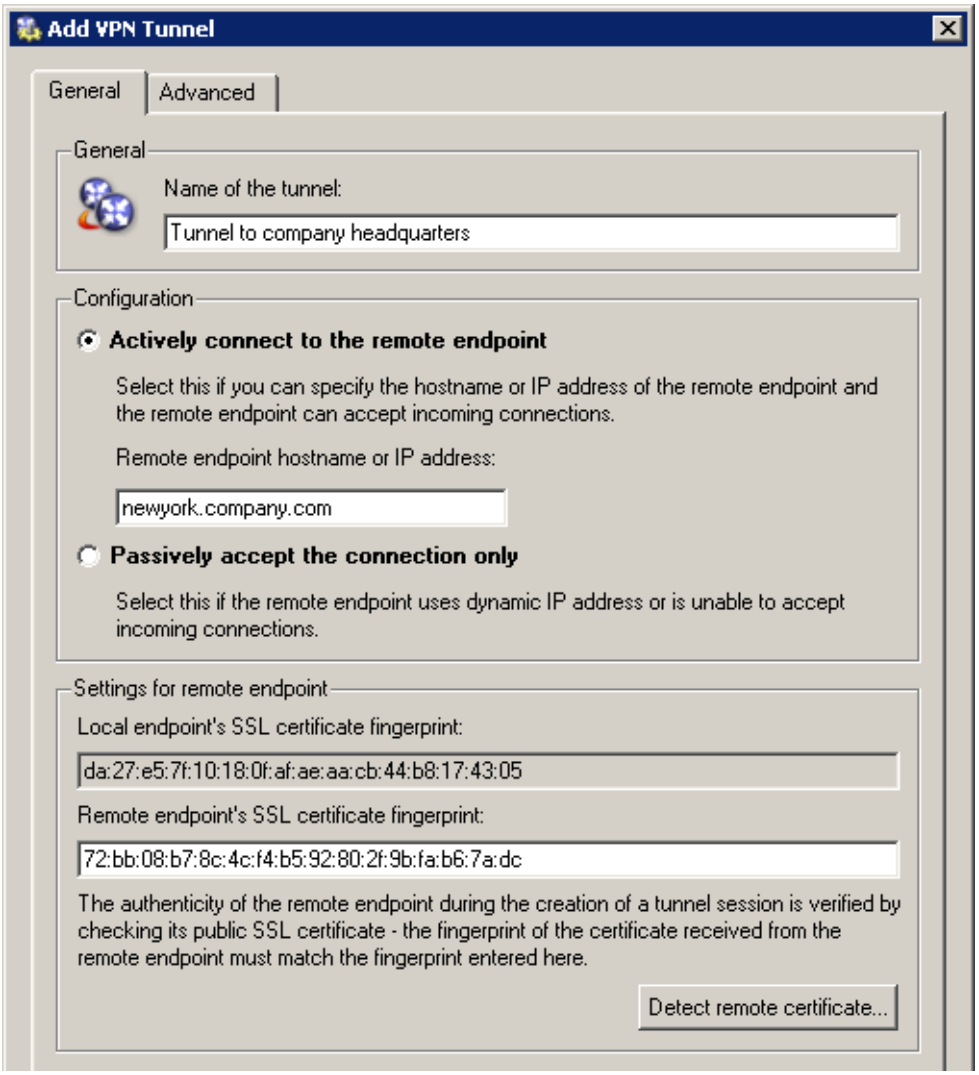

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to company headquarters
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
newyork.company.com
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
Remote endpoint's SSL certificate fingerprint:
72:bb:08:b7:8c:4c:f4:b5:92:80:2f:9b:fa:b6:7a:dc
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.29 Filial office — definition of VPN tunnel for the headquarters

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN Firewall Tunnel to company headquarters	LAN Firewall Tunnel to company he	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
Service Kerio VPN	Internet	Firewall	Kerio VPN	✓	

Figure 21.30 Filial office — final traffic rules

Note: It is not necessary to perform any other customization of traffic rules. The required restrictions should be already set in the traffic policy at the server of the headquarters.

VPN test

Configuration of the VPN tunnel has been completed by now. At this point, it is recommended to test availability of the remote hosts from each end of the tunnel (from both local networks).

For example, the `ping` or/and `tracert` operating system commands can be used for this testing. It is recommended to test availability of remote hosts both through IP addresses and DNS names.

If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

If an IP address is tested successfully and an error is reported (*Unknown host*) when a corresponding DNS name is tested, then check configuration of the DNS.

21.6 Example of a more complex Kerio VPN configuration

In this chapter, an example of a more complex VPN configuration is provided where redundant routes arise between interconnected private networks (i.e. multiple routes exist between two networks that can be used for transfer of packets).

The only difference of *Kerio VPN* configuration between this type and VPN with no redundant routes (see chapter 21.5) is setting of routing between endpoints of individual tunnels. In such a case, it is necessary to set routing between individual endpoints of VPN tunnels by hand. Automatic route exchange is inconvenient since *Kerio VPN* uses no routing protocol and the route exchange is based on comparison of routing tables at individual endpoints of the VPN tunnel (see also chapter 21.4). If the automatic exchange is applied, the routing will not be ideal!

For better reference, the configuration is here described by an example of a company with a headquarters and two filial offices with their local private network interconnected by VPN tunnels (so called triangle pattern). This example can be then adapted and applied to any number of interconnected private networks.

The example focuses configuration of VPN tunnels and correct setting of routing between individual private networks (it does not include access restrictions). Access restrictions options within VPN are described by the example in chapter 21.5.

Specification

The network follows the pattern shown in figure 21.31.

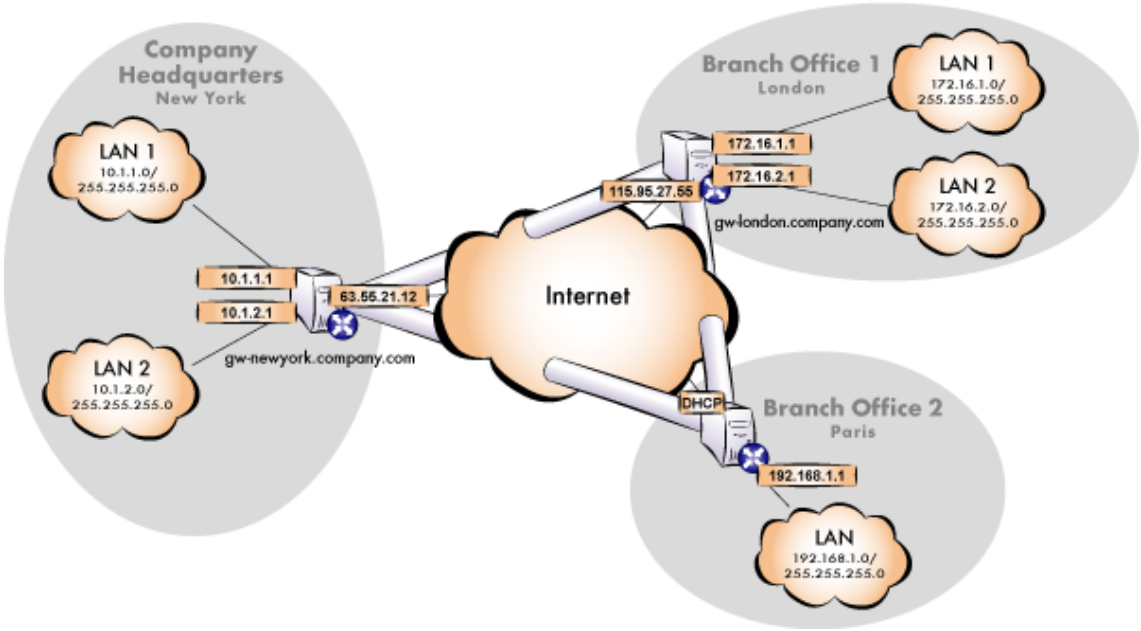


Figure 21.31 Example of a VPN configuration — a company with two filials

The server (default gateway) uses the fixed IP address `63.55.21.12` (DNS name is `gw-newyork.company.com`). The server of one filial uses the IP address `115.95.27.55` (DNS name `gw-london.company.com`), the other filial's server uses a dynamic IP address assigned by the ISP.

The headquarters uses the DNS domain `company.com`, filials use subdomains `santaclara.company.com` and `newyork.company.com`. Configuration of individual local networks and the IP addresses used are shown in the figure.

Common method

The following actions must be taken in all local networks (i.e. in the main office and both filials):

1. *WinRoute* in version `6.1.0` or higher must be installed at the default gateway. Older versions do not allow setting of routing for VPN tunnels. Therefore, they cannot be used for this VPN configuration (see figure 21.31).

Note: For *each* installation of *WinRoute*, a separate license for corresponding number of users is required! For details see chapter 4.

2. Configure and test connection of the local network to the Internet. Hosts in the local network must use the *WinRoute* host's IP address as the default gateway and as the primary DNS server.

   If it is a new (clean) *WinRoute* installation, it is possible to use the traffic rule wizard (refer to chapter 6.1).

   For detailed description of basic configuration of *WinRoute* and of the local network, refer to the *Kerio WinRoute Firewall — Step By Step* document.

3. In configuration of *DNS Forwarder*, set DNS forwarding rules for domains of the other filials. This enables to access hosts in the remote networks by using their DNS names (otherwise, it is necessary to specify remote hosts by IP addresses).

   To provide correct forwarding of DNS requests from a *WinRoute* host, it is necessary to use an IP address of a network device belonging to the host as the primary DNS server. In *DNS Forwarder* configuration, at least one DNS server must be specified to which DNS queries for other domains (typically the DNS server of the ISP).

   Note: For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the `hosts` file (if they use IP addresses) or enable co-operation of the *DNS Forwarder* with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 5.3.

4. In the *Interfaces* section, allow the VPN server and set its SSL certificate if necessary. Note the fingerprint of the server's certificate for later use (it will be required for configuration of the VPN tunnels in the other filials).

   Check whether the automatically selected VPN subnet does not collide with any local subnet in any filial and select another free subnet if necessary.

   Note: With respect to the complexity of this VPN configuration, it is recommended to reserve three free subnets in advance that can later be assigned to individual VPN servers.

5. Define the VPN tunnel to one of the remote networks. The passive endpoint of the tunnel must be created at a server with fixed public IP address. Only active endpoints of VPN tunnels can be created at servers with dynamic IP address.

   Set routing (define custom routes) for the tunnel. Select the *Use custom routes only* option and specify all subnets of the remote network in the custom routes list.

If the remote endpoint of the tunnel has already been defined, check whether the tunnel was created. If not, refer to the *Error* log, check fingerprints of the certificates and also availability of the remote server.

6. Follow the same method to define a tunnel and set routing to the other remote network.

7. Allow traffic between the local and the remote networks. To allow any traffic, just add the created VPN tunnels to the *Source* and *Destination* items in the *Local traffic* rule. Access restrictions options within VPN are described by the example in chapter 21.5.

8. Test reachability of remote hosts in both remote networks. To perform the test, use the `ping` and `tracert` system commands. Test availability of remote hosts both through IP addresses and DNS names.

   If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

   If an IP address is tested successfully and an error is reported (*Unknown host*) when a corresponding DNS name is tested, then check configuration of the DNS.

The following sections provide detailed description of the *Kerio VPN* configuration both for the headquarter and the filial offices.

Headquarters configuration

1. Install *WinRoute* (version `6.1.0` or higher) at the default gateway of the headquarters network.

2. Use *Network Rules Wizard* (see chapter 6.1) to configure the basic traffic policy in *WinRoute*. To keep the example as simple as possible, it is supposed that the access from the local network to the Internet is not restricted, i.e. that access to all services is allowed in step 4.

   In step 5, select *Create rules for Kerio VPN server*. Status of the *Create rules for Kerio Clientless SSL-VPN* option is irrelevant (this example does not include *Clientless SSL-VPN* interface's issues).

   This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

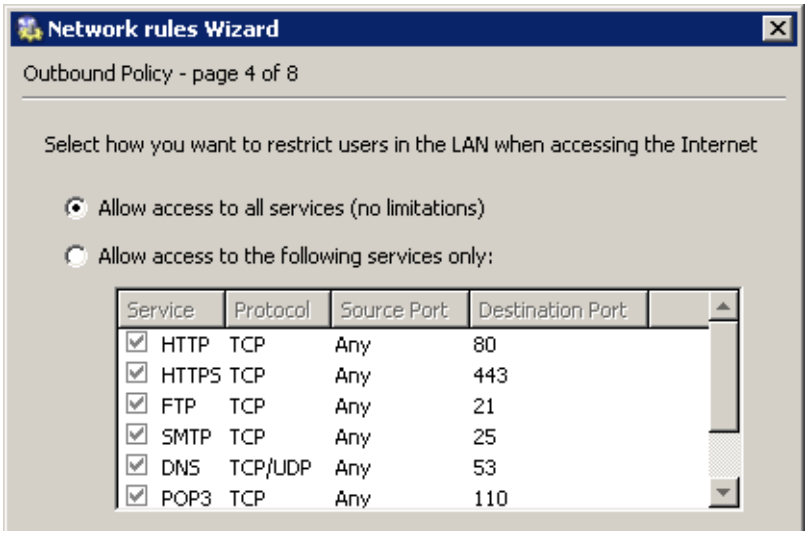

Network rules Wizard
Outbound Policy - page 4 of 8
Select how you want to restrict users in the LAN when accessing the Internet
Allow access to all services (no limitations)
Allow access to the following services only:
Service
Protocol
Source Port
Destination Port
HTTP TCP Any 80
HTTPS TCP Any 443
FTP TCP Any 21
SMTP TCP Any 25
DNS TCP/UDP Any 53
POP3 TCP Any 110

Figure 21.32 Headquarters — no restrictions are applied to accessing the Internet from the LAN

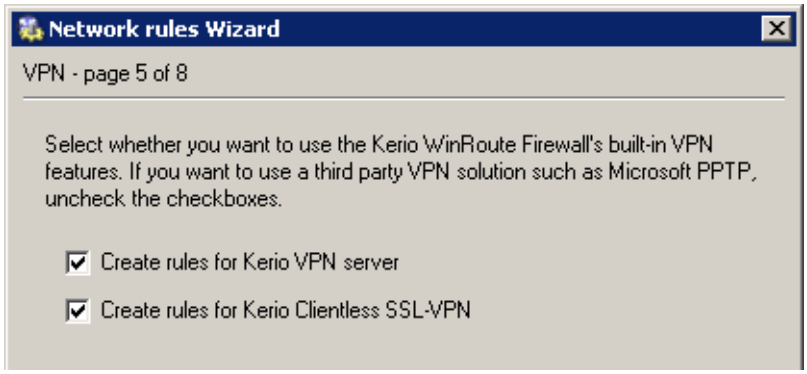

Network rules Wizard
VPN - page 5 of 8
Select whether you want to use the Kerio WinRoute Firewall's built-in VPN features. If you want to use a third party VPN solution such as Microsoft PPTP, uncheck the checkboxes.
Create rules for Kerio VPN server
Create rules for Kerio Clientless SSL-VPN

Figure 21.33 Headquarter — creating default traffic rules for Kerio VPN

Name	Source	Destination	Service	Action	Translation
Local Traffic	Dial-In LAN 1 LAN 2 Firewall VPN clients	Dial-In LAN 1 LAN 2 Firewall VPN clients	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.34 Headquarter — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:

   - In configuration of the *DNS Forwarder* in *WinRoute*, specify DNS servers to which DNS queries which are not addressed to the `company.com` domain will be forwarded (primary and secondary DNS server of the Internet connection provider by default).

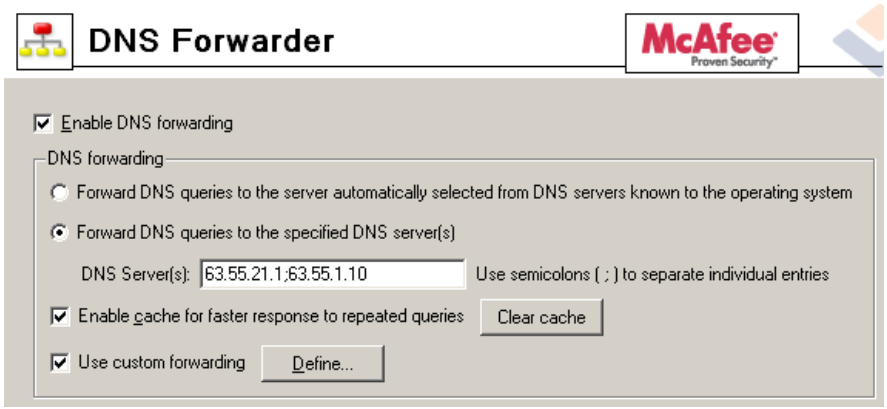

DNS Forwarder
McAfee
Proven Security
Enable DNS forwarding
DNS forwarding
Forward DNS queries to the server automatically selected from DNS servers known to the operating system
Forward DNS queries to the specified DNS server(s)
DNS Server(s):
63.55.21.1;63.55.1.10
Use semicolons (;) to separate individual entries
Enable cache for faster response to repeated queries
Clear cache
Use custom forwarding
Define...

Figure 21.35 Headquarter — DNS forwarder configuration

   - Enable the *Use custom forwarding* option and define rules for names in the `filial1.company.com` and `filial2.company.com` domains. To specify the forwarding DNS server, always use the IP address of the *WinRoute* host's inbound interface connected to the local network at the remote side of the tunnel.

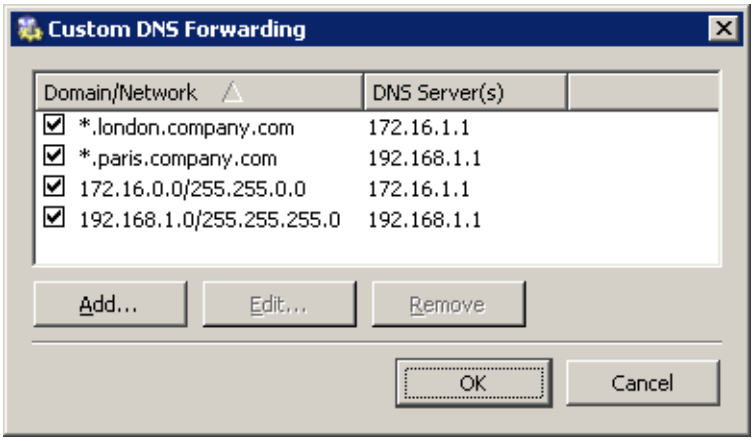


Figure 21.36 Headquarter — DNS forwarding settings

- Set the IP address of this interface (`10.1.1.1`) as a primary DNS server for the *WinRoute* host's interface connected to the *LAN 1* local network. It is not necessary to set DNS at the interface connected to *LAN 2*.

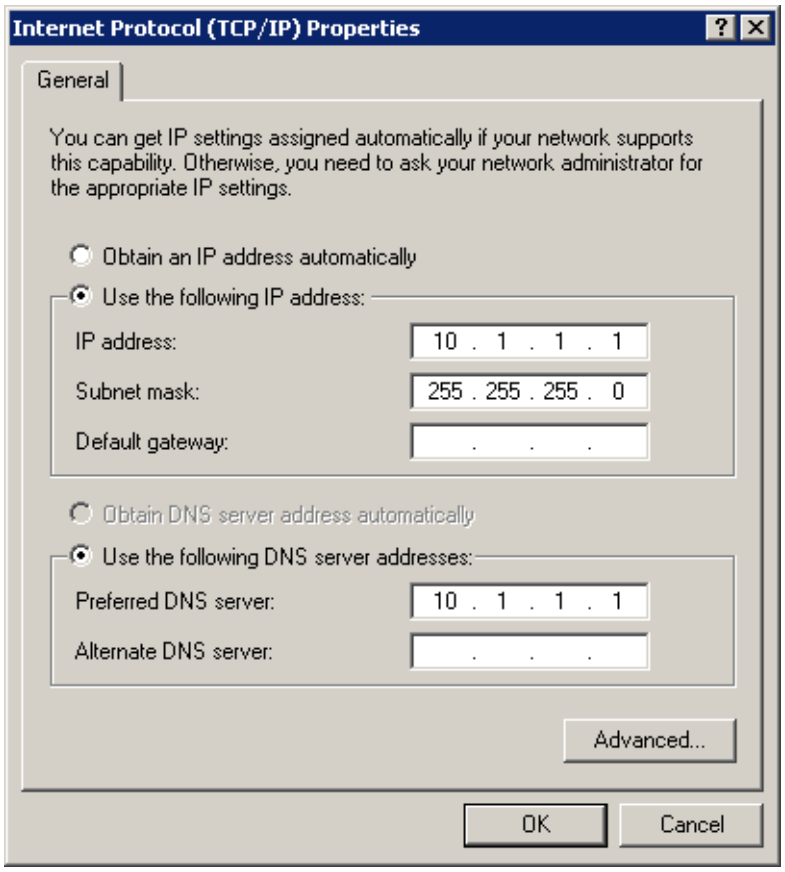

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 1 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 1 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Figure 21.37 Headquarter — TCP/IP configuration
at a firewall's interface connected to the local network

- Set the IP address `10.1.1.1` as a primary DNS server also for the other hosts.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: A free subnet which has been selected is now specified automatically in the *VPN network* and *Mask* entries. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

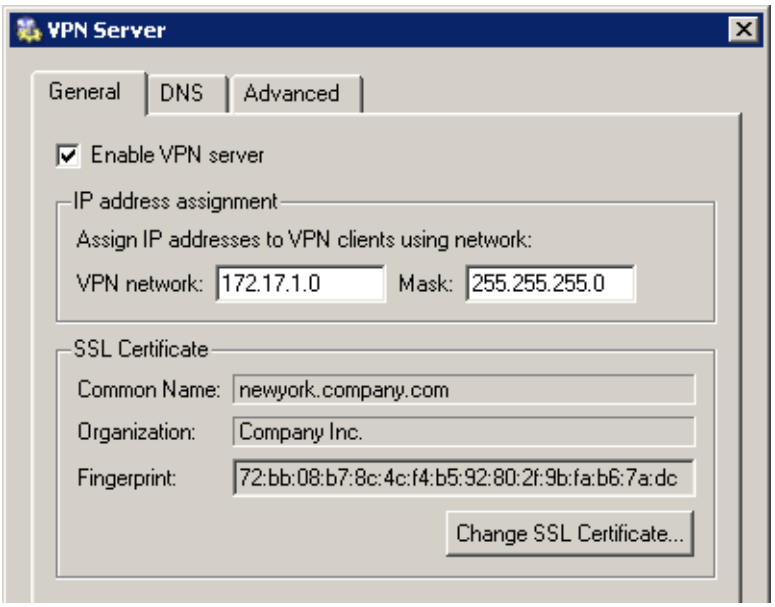


Figure 21.38 Headquarters — VPN server configuration

For a detailed description on the VPN server configuration, refer to chapter 21.1.

5. Create a passive endpoint of the VPN tunnel connected to the *London* filial. Use the fingerprint of the VPN server of the *London* filial office as a specification of the fingerprint of the remote SSL certificate.

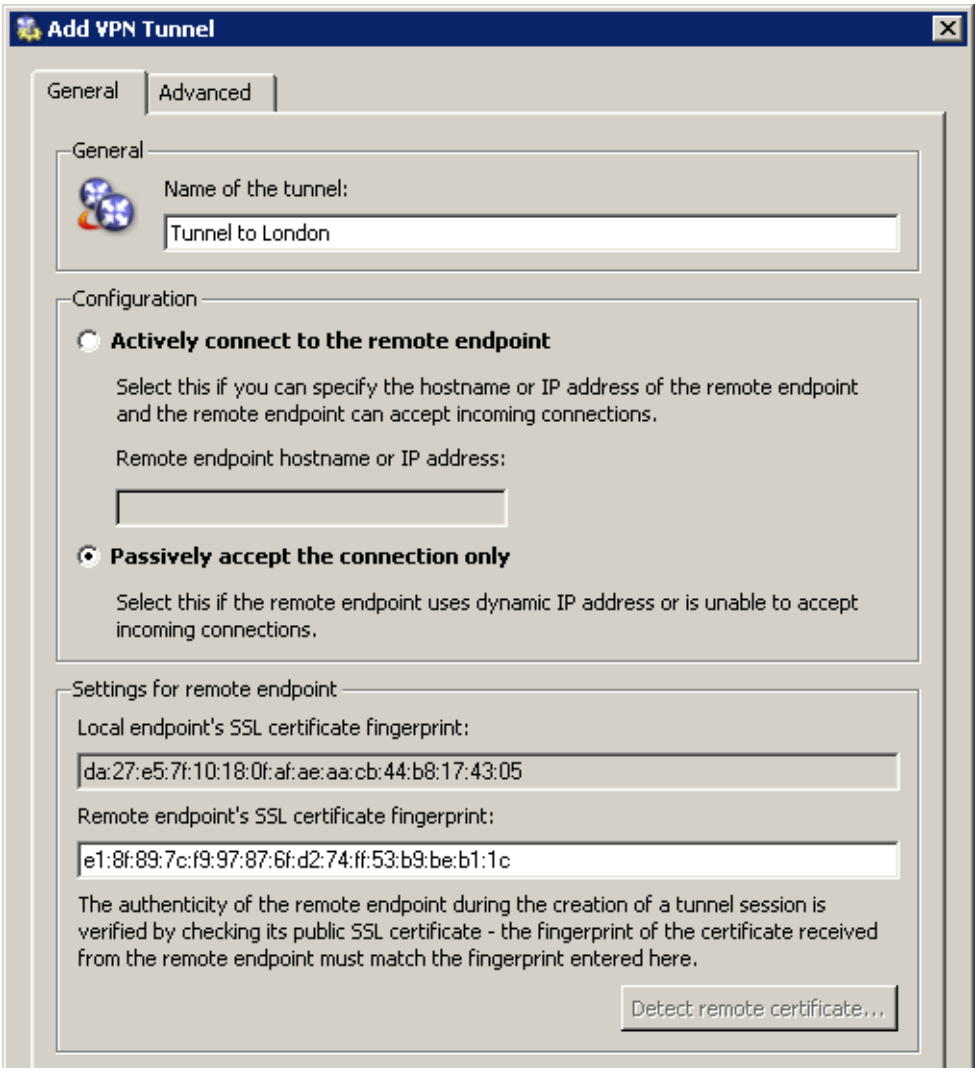

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to London
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
Remote endpoint's SSL certificate fingerprint:
e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.39 Headquarter — definition of VPN tunnel for the London filial

On the *Advanced* tab, select the *Use custom routes only* option and set routes to the subnets at the remote endpoint of the tunnel (i.e. in the *London* filial).

Warning: In case that the VPN configuration described here is applied see figure 21.31) it is *not recommended* to use automatically provided routes! In case of an automatic exchange of routes, the routing within the VPN is not be ideal (for example, any traffic between the *headquarters* and the *Paris* filial office is routed via

the *London* filial whereas the tunnel between the *headquarters* and the *Paris* office stays waste.

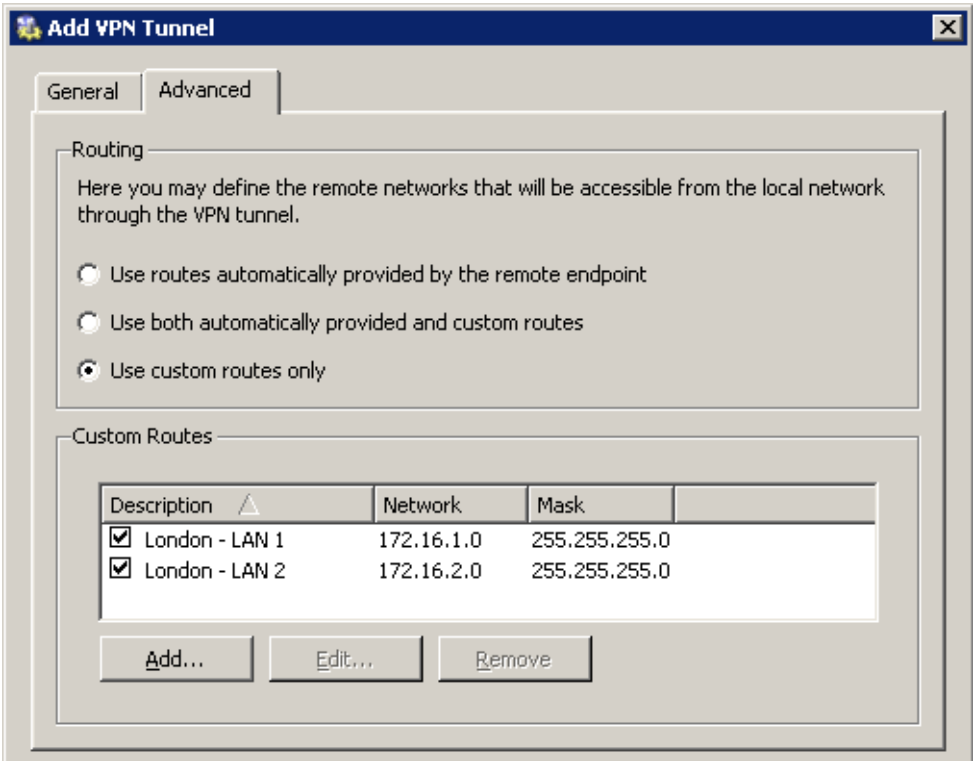


Figure 21.40 The headquarters — routing configuration for the tunnel connected to the London filial

6. Use the same method to create a passive endpoint for the tunnel connected to the *Paris* filial.

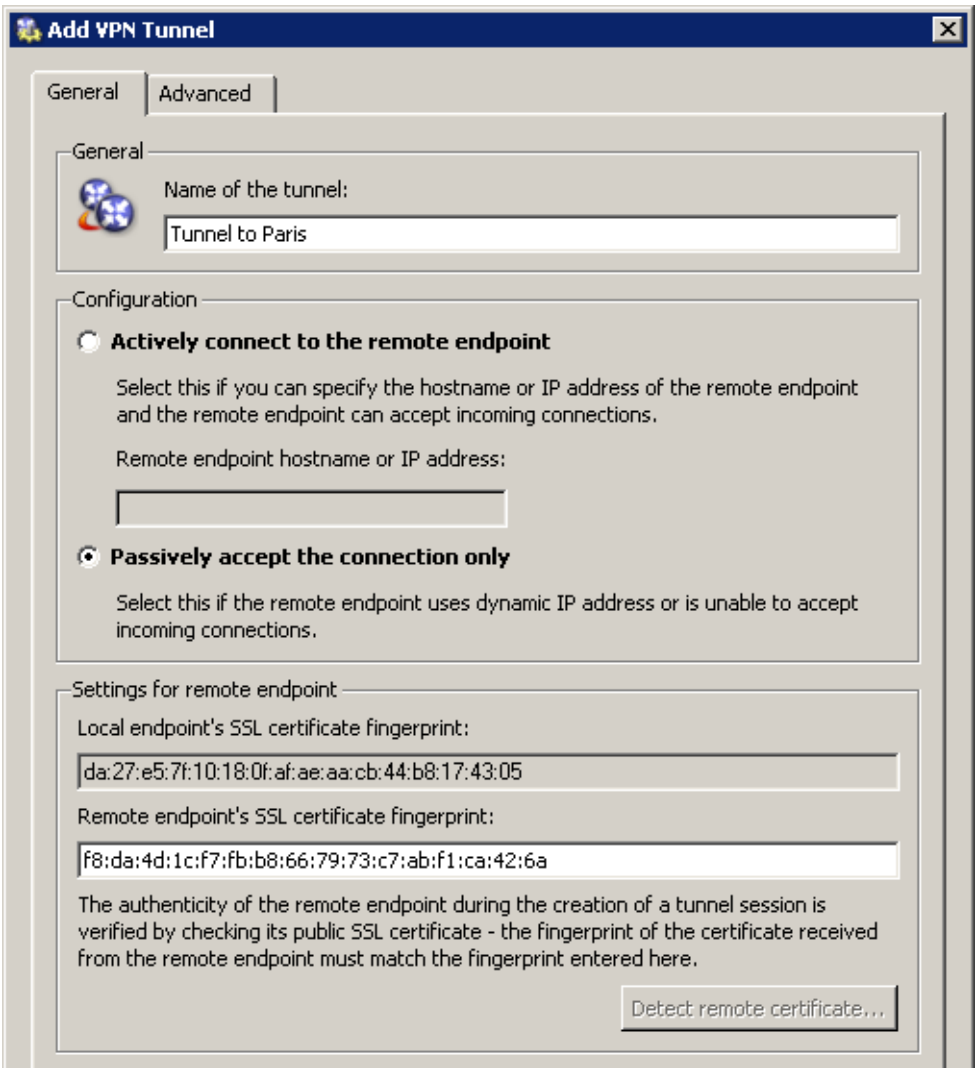

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to Paris
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
Remote endpoint's SSL certificate fingerprint:
f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.41 The headquarters — definition of VPN tunnel for the Paris filial

On the *Advanced* tab, select the *Use custom routes only* option and set routes to the subnets at the remote endpoint of the tunnel (i.e. in the *Paris* filial).

7. Add the new VPN tunnels into the *Local Traffic* rule.

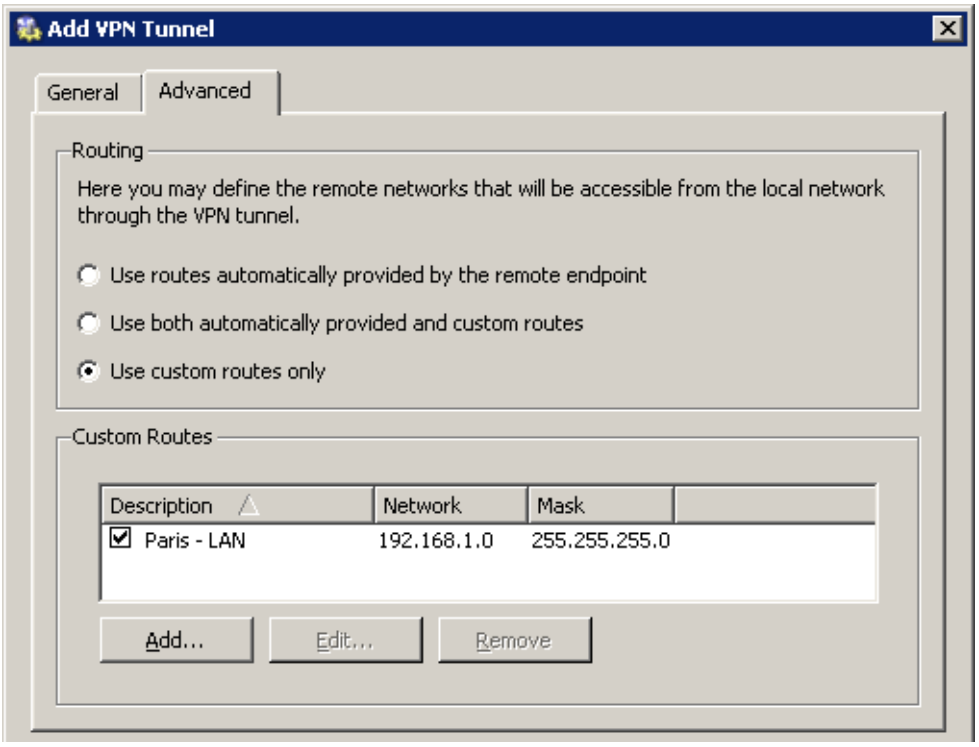


Figure 21.42 The headquarters — routing configuration for the tunnel connected to the Paris filial

Name	Source	Destination	Service	Action	Translation
Local Traffic	Dial-In LAN 1 LAN 2 Firewall VPN clients Tunnel to London Tunnel to Paris	Dial-In LAN 1 LAN 2 Firewall VPN clients Tunnel to London Tunnel to Paris	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
Service Kerio VPN	Internet	Firewall	Kerio VPN	✓	

Figure 21.43 Headquarter — final traffic rules

Configuration of the London filial

1. Install *WinRoute* (version `6.1.0` or higher) at the default gateway of the filial's network.

2. Use *Network Rules Wizard* (see chapter 6.1) to configure the basic traffic policy in *WinRoute*. To keep the example as simple as possible, it is supposed that the access from the local network to the Internet is not restricted, i.e. that access to all services is allowed in step 4.

   In step 5 of the wizard, select the *Create rules for Kerio VPN server* option (setting of the *Create rules for Kerio Clientless SSL-VPN* option is not regarded here).

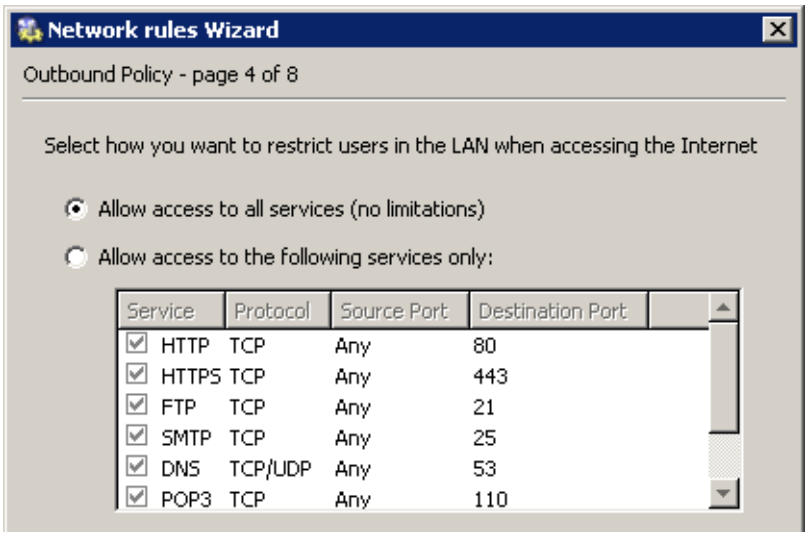

Network rules Wizard
Outbound Policy - page 4 of 8
Select how you want to restrict users in the LAN when accessing the Internet
Allow access to all services (no limitations)
Allow access to the following services only:
Service
Protocol
Source Port
Destination Port
HTTP TCP Any 80
HTTPS TCP Any 443
FTP TCP Any 21
SMTP TCP Any 25
DNS TCP/UDP Any 53
POP3 TCP Any 110

Figure 21.44 The London filial — no restrictions are applied to accessing the Internet from the LAN

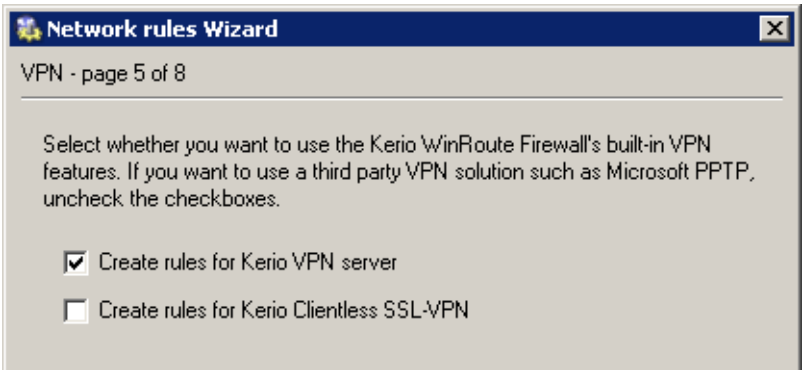

Network rules Wizard
VPN - page 5 of 8
Select whether you want to use the Kerio WinRoute Firewall's built-in VPN features. If you want to use a third party VPN solution such as Microsoft PPTP, uncheck the checkboxes.
Create rules for Kerio VPN server
Create rules for Kerio Clientless SSL-VPN

Figure 21.45 The London filial office — creating default traffic rules for Kerio VPN

This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

Name	Source	Destination	Service	Action	Translation
Local Traffic	Dial-In LAN 1 LAN 2 Firewall VPN clients	Dial-In LAN 1 LAN 2 Firewall VPN clients	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
VPN server connections	Internet	Firewall	Kerio VPN	✓	

Figure 21.46 The London filial office — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:

   - In configuration of the *DNS Forwarder* in *WinRoute*, specify DNS servers to which DNS queries which are not addressed to the `company.com` domain will be forwarded (primary and secondary DNS server of the Internet connection provider by default).

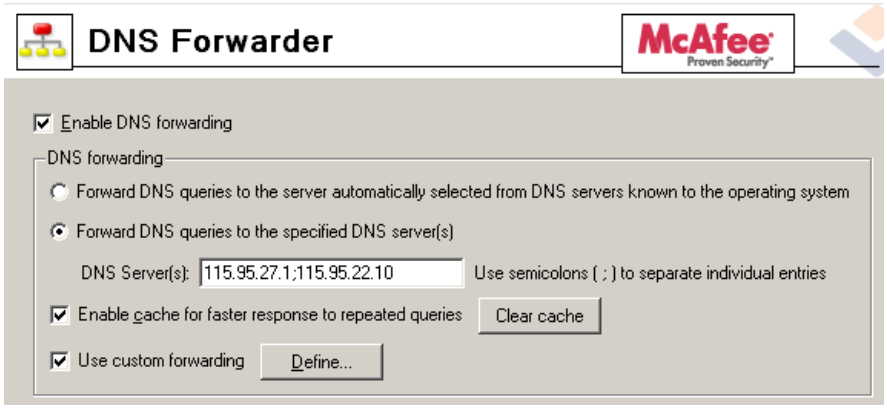

DNS Forwarder
McAfee
Proven Security
Enable DNS forwarding
DNS forwarding
Forward DNS queries to the server automatically selected from DNS servers known to the operating system
Forward DNS queries to the specified DNS server(s)
DNS Server(s):
115.95.27.1;115.95.22.10
Use semicolons (;) to separate individual entries
Enable cache for faster response to repeated queries
Clear cache
Use custom forwarding
Define...

Figure 21.47 The London filial office — DNS forwarder configuration

   - Enable the *Use custom forwarding* option and define rules for names in the `company.com` and `filial2.company.com` domains. To specify the forwarding DNS server, always use the IP address of the *WinRoute* host's inbound interface connected to the local network at the remote side of the tunnel.

   - Set the IP address of this interface (`172.16.1.1`) as a primary DNS server for the *WinRoute* host's interface connected to the *LAN 1* local network. It is not necessary to set DNS at the interface connected to *LAN 2*.

   - Set the IP address `172.16.1.1` as a primary DNS server also for the other hosts.

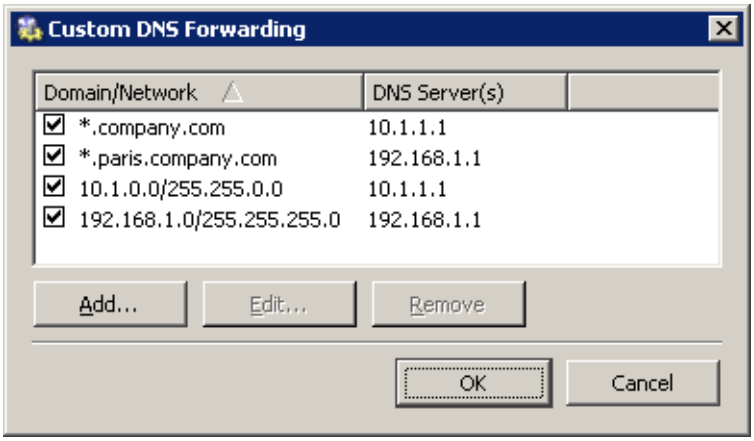


Figure 21.48 The London filial office — DNS forwarding settings

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: A free subnet which has been selected is now specified automatically in the *VPN network* and *Mask* entries. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

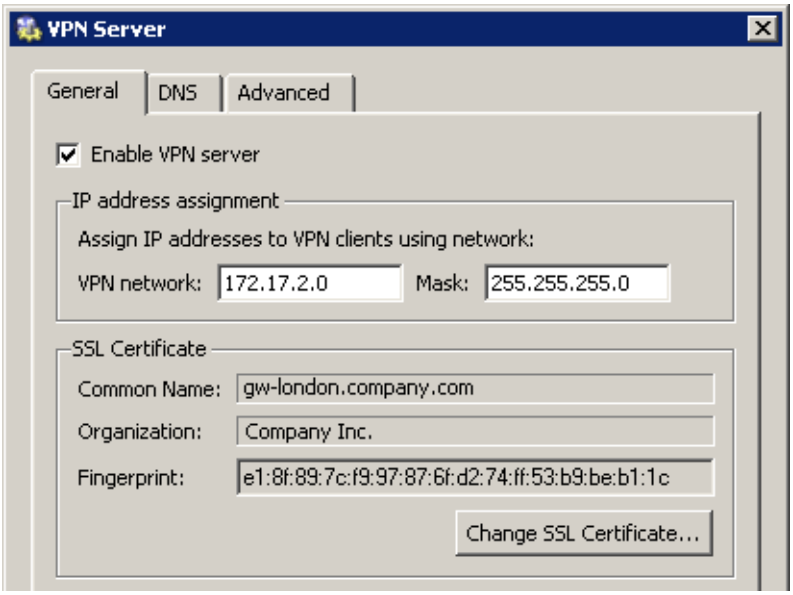


Figure 21.49 The London filial office — VPN server configuration

For a detailed description on the VPN server configuration, refer to chapter 21.1.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (`newyork.company.com`). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.

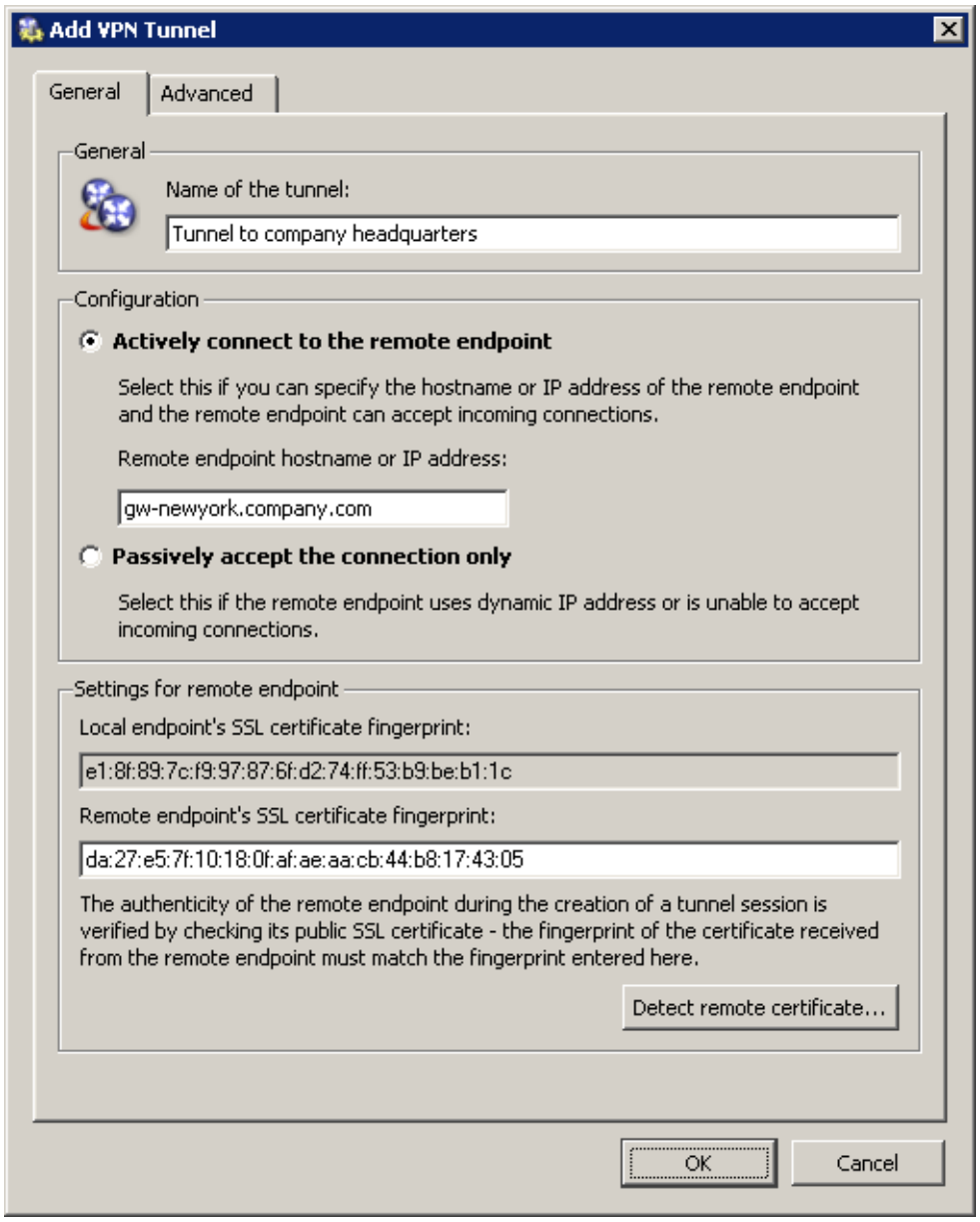

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to company headquarters
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
gw-newyork.company.com
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c
Remote endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...
OK
Cancel

Figure 21.50 The London filial office — definition of VPN tunnel for the headquarters

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *headquarters'* local networks.

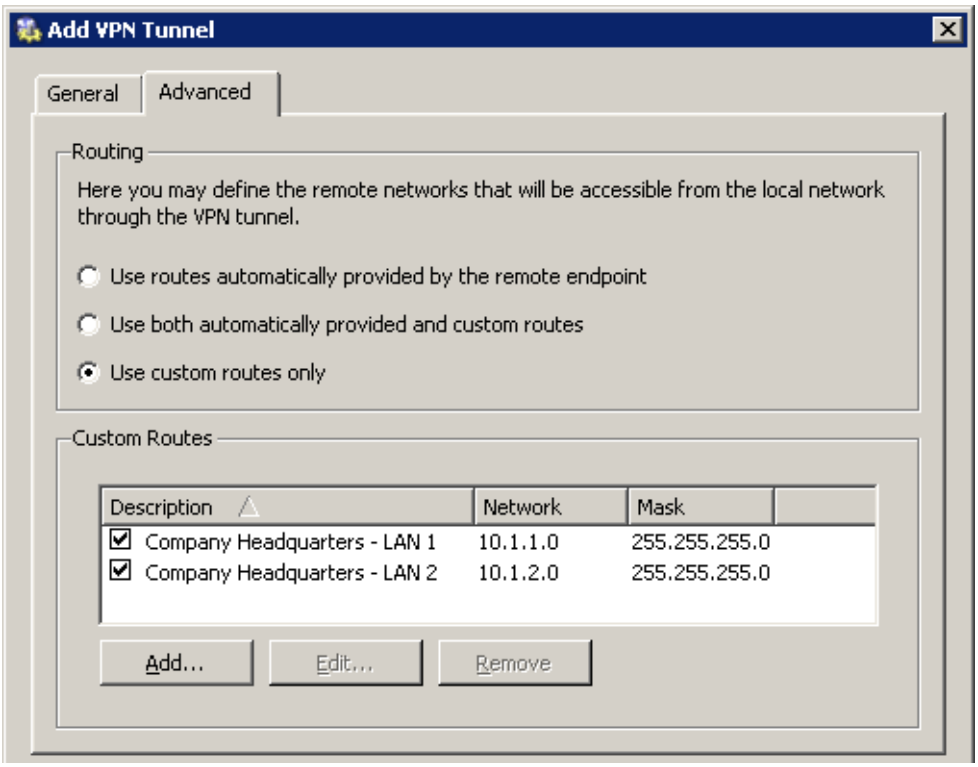


Figure 21.51 The London filial — routing configuration for the tunnel connected to the headquarters

At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the *Connected* status will be reported in the *Adapter info* column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server — in our example, the `ping gw-newyork.company.com` command can be used at the London branch office server.

6. Create a passive endpoint of the VPN tunnel connected to the *Paris* filial. Use the fingerprint of the VPN server of the *Paris* filial office as a specification of the fingerprint of the remote SSL certificate.

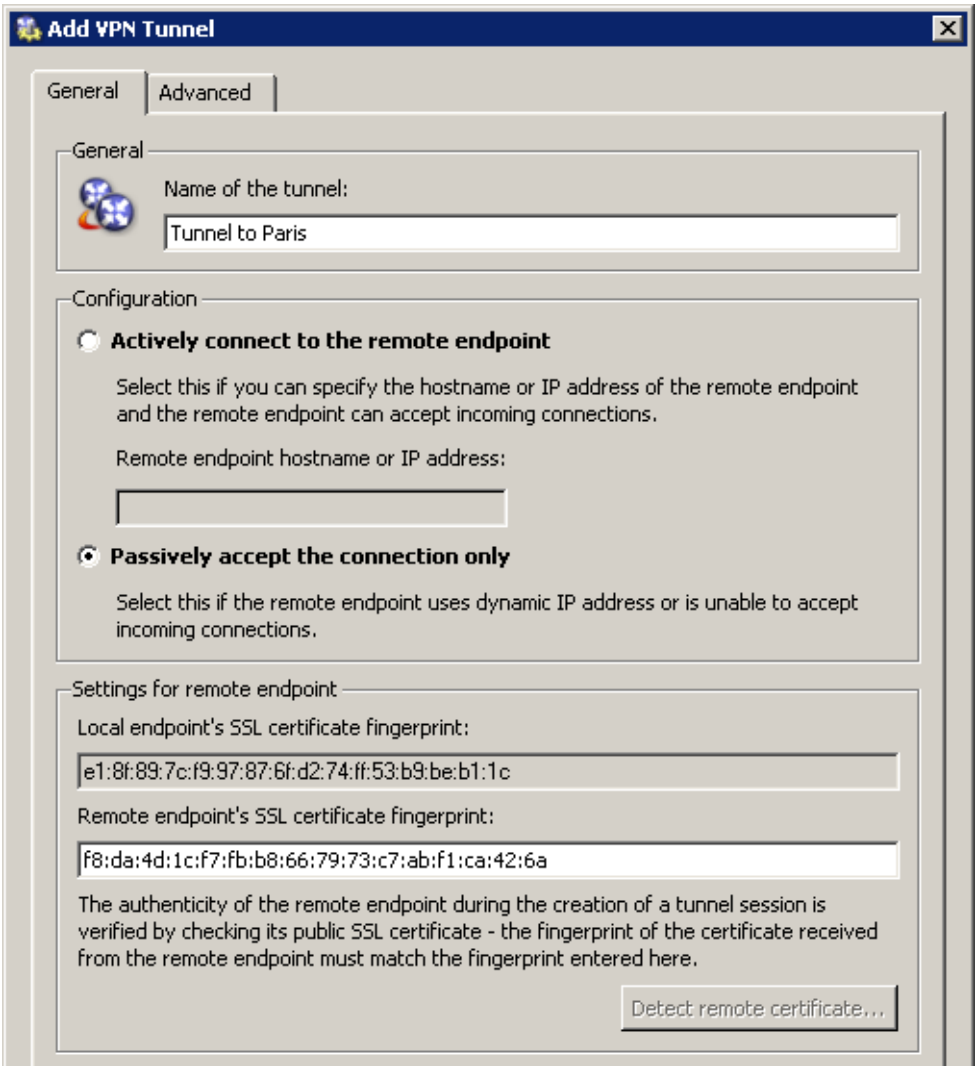

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to Paris
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c
Remote endpoint's SSL certificate fingerprint:
f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.52 The London filial office — definition of VPN tunnel for the Paris filial office

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *Paris'* local networks.

7. Add the new VPN tunnels into the *Local Traffic* rule. It is also possible to remove the *Dial-In* interface and the *VPN clients* group from this rule (supposing that all VPN clients connect to the headquarters' server).

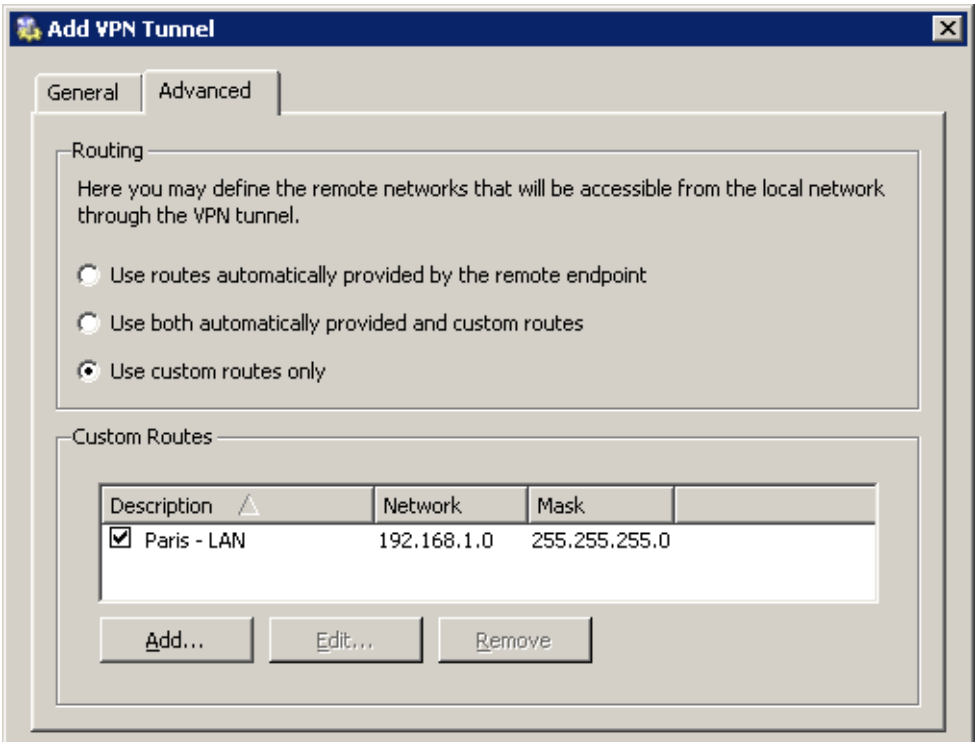


Figure 21.53 The London filial — routing configuration for the tunnel connected to the Paris branch office

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN 1 LAN 2 Firewall Tunnel to company headquarters Tunnel to Paris	LAN 1 LAN 2 Firewall Tunnel to company hea Tunnel to Paris	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
Service Kerio VPN	Internet	Firewall	Kerio VPN	✓	

Figure 21.54 The London filial office — final traffic rules

Configuration of the Paris filial

1. Install *WinRoute* (version `6.1.0` or higher) at the default gateway of the filial's network.

2. Use *Network Rules Wizard* (see chapter 6.1) to configure the basic traffic policy in *WinRoute*. To keep the example as simple as possible, it is supposed that the access from the local network to the Internet is not restricted, i.e. that access to all services is allowed in step 4.

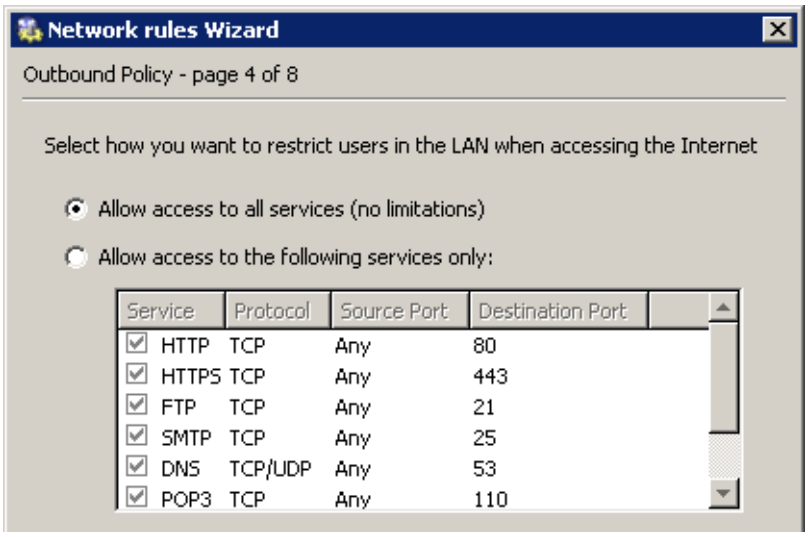

Network rules Wizard
Outbound Policy - page 4 of 8
Select how you want to restrict users in the LAN when accessing the Internet
Allow access to all services (no limitations)
Allow access to the following services only:
Service
Protocol
Source Port
Destination Port
HTTP TCP Any 80
HTTPS TCP Any 443
FTP TCP Any 21
SMTP TCP Any 25
DNS TCP/UDP Any 53
POP3 TCP Any 110

Figure 21.55 The Paris filial — no restrictions are applied to accessing the Internet from the LAN

In this case, it would be meaningless to create rules for the *Kerio VPN server* and/or the *Kerio Clientless SSL-VPN*, since the server uses a dynamic public IP address). Therefore, leave these options disabled in step 5.

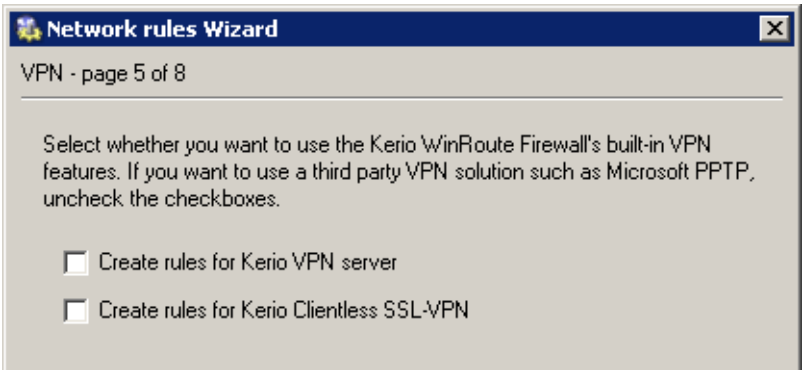

Network rules Wizard
VPN - page 5 of 8
Select whether you want to use the Kerio WinRoute Firewall's built-in VPN features. If you want to use a third party VPN solution such as Microsoft PPTP, uncheck the checkboxes.
Create rules for Kerio VPN server
Create rules for Kerio Clientless SSL-VPN

Figure 21.56 The Paris filial — default rules for Kerio VPN will not be created

3. Customize DNS configuration as follows:

   - In configuration of the *DNS Forwarder* in *WinRoute*, specify DNS servers to which DNS queries which are not addressed to the `company.com` domain will be forwarded (primary and secondary DNS server of the Internet connection provider by default).

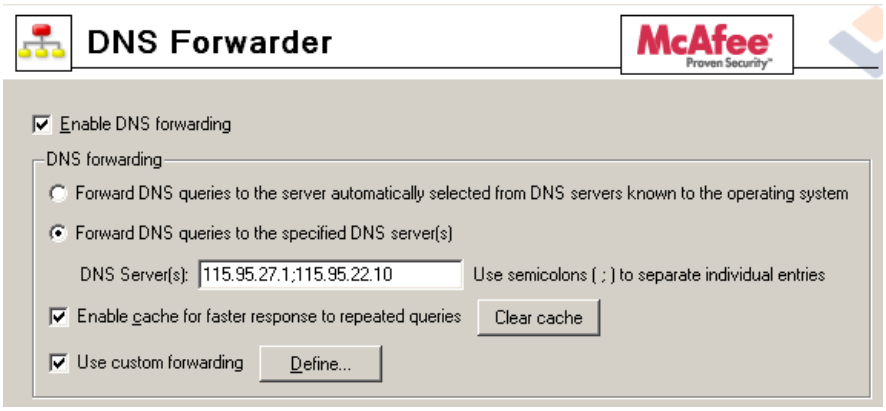

DNS Forwarder
McAfee
Proven Security
Enable DNS forwarding
DNS forwarding
Forward DNS queries to the server automatically selected from DNS servers known to the operating system
Forward DNS queries to the specified DNS server(s)
DNS Server(s):
115.95.27.1;115.95.22.10
Use semicolons (;) to separate individual entries
Enable cache for faster response to repeated queries
Clear cache
Use custom forwarding
Define...

Figure 21.57 The Paris filial office — DNS forwarder configuration

   - Enable the *Use custom forwarding* option and define rules for names in the `company.com` and `filial1.company.com` domains. Specify the server for DNS forwarding by the IP address of the remote firewall host's interface (i.e. interface connected to the local network at the other end of the tunnel).

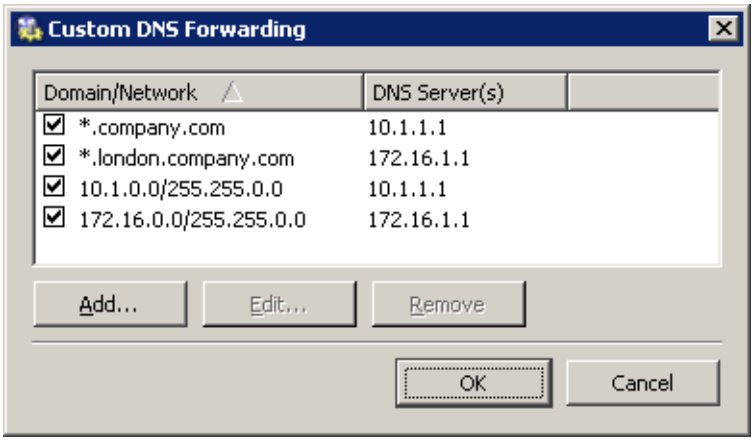


Figure 21.58 The Paris filial office — DNS forwarding settings

- Set the IP address of this interface (`172.16.1.1`) as a primary DNS server for the *WinRoute* host's interface connected to the *LAN 1* local network. It is not necessary to set DNS at the interface connected to *LAN 2*.
- Set the IP address `172.16.1.1` as a primary DNS server also for the other hosts.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: A free subnet which has been selected is now specified automatically in the *VPN network* and *Mask* entries. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

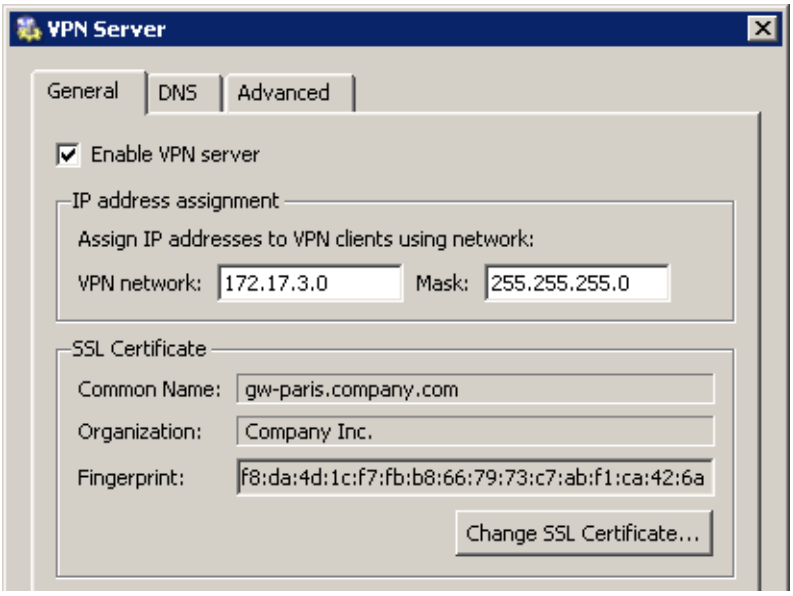


Figure 21.59 The Paris filial office — VPN server configuration

For a detailed description on the VPN server configuration, refer to chapter 21.1.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (`newyork.company.com`). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.

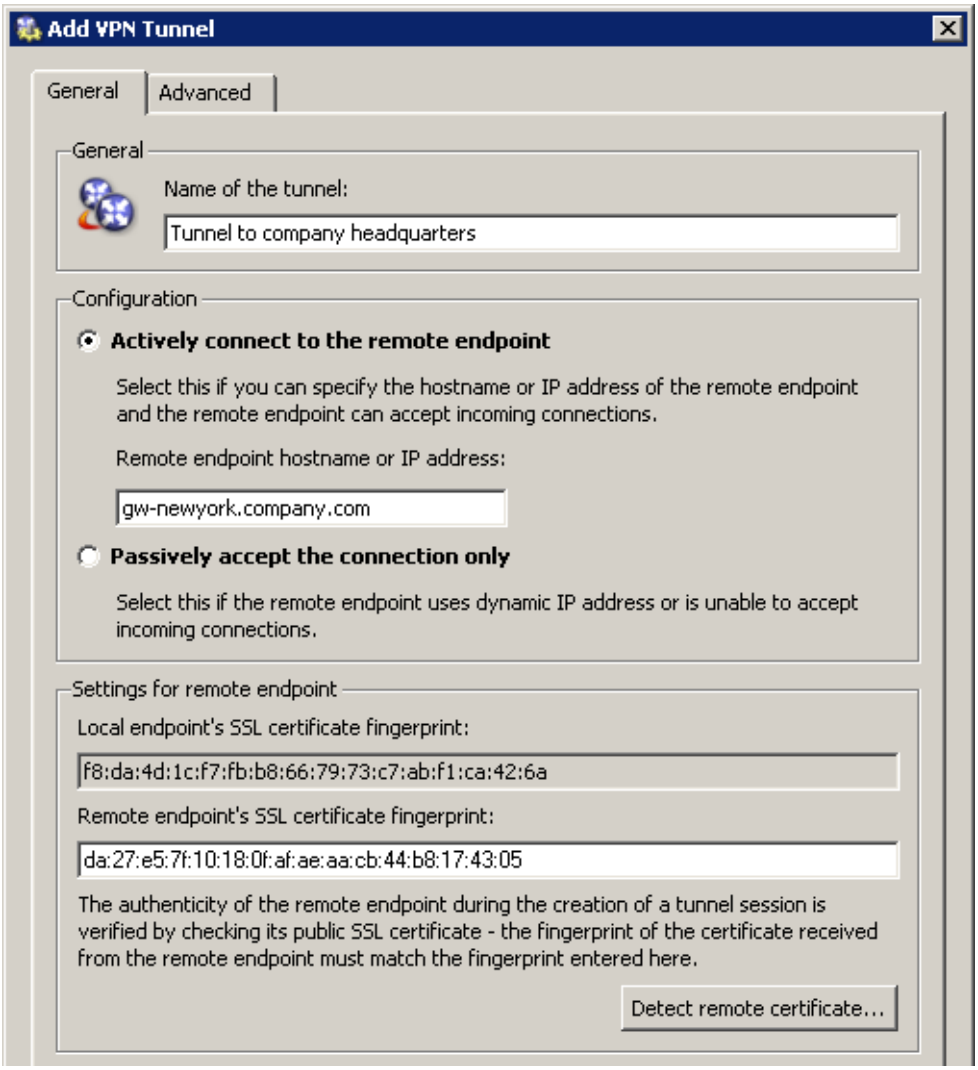

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to company headquarters
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
gw-newyork.company.com
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a
Remote endpoint's SSL certificate fingerprint:
da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...

Figure 21.60 The Paris filial office — definition of VPN tunnel for the headquarters

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *headquarters'* local networks.

At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the *Connected* status will be reported in the *Adapter info* column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability

of the remote server — in our example, the `ping gw-sanfrancisco.company.com` command can be used at the Paris branch office server.

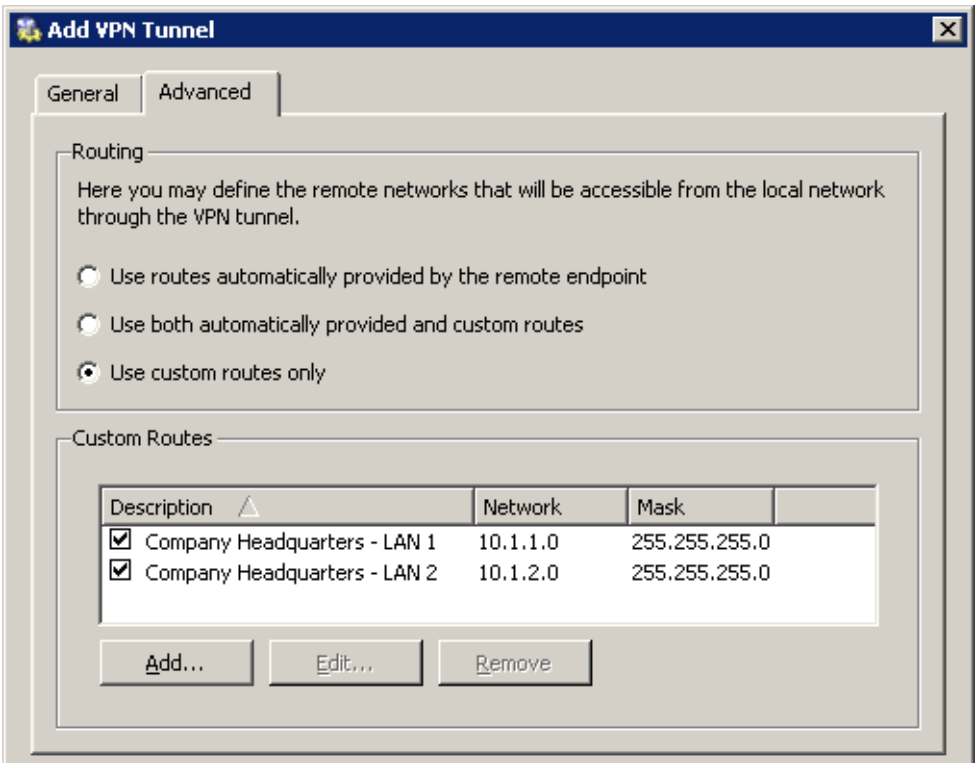


Figure 21.61 The Paris filial — routing configuration for the tunnel connected to the headquarters

6. Create an active endpoint of the tunnel connected to *London* (server `gw-london.company.com`). Use the fingerprint of the VPN server of the *London* filial office as a specification of the fingerprint of the remote SSL certificate.

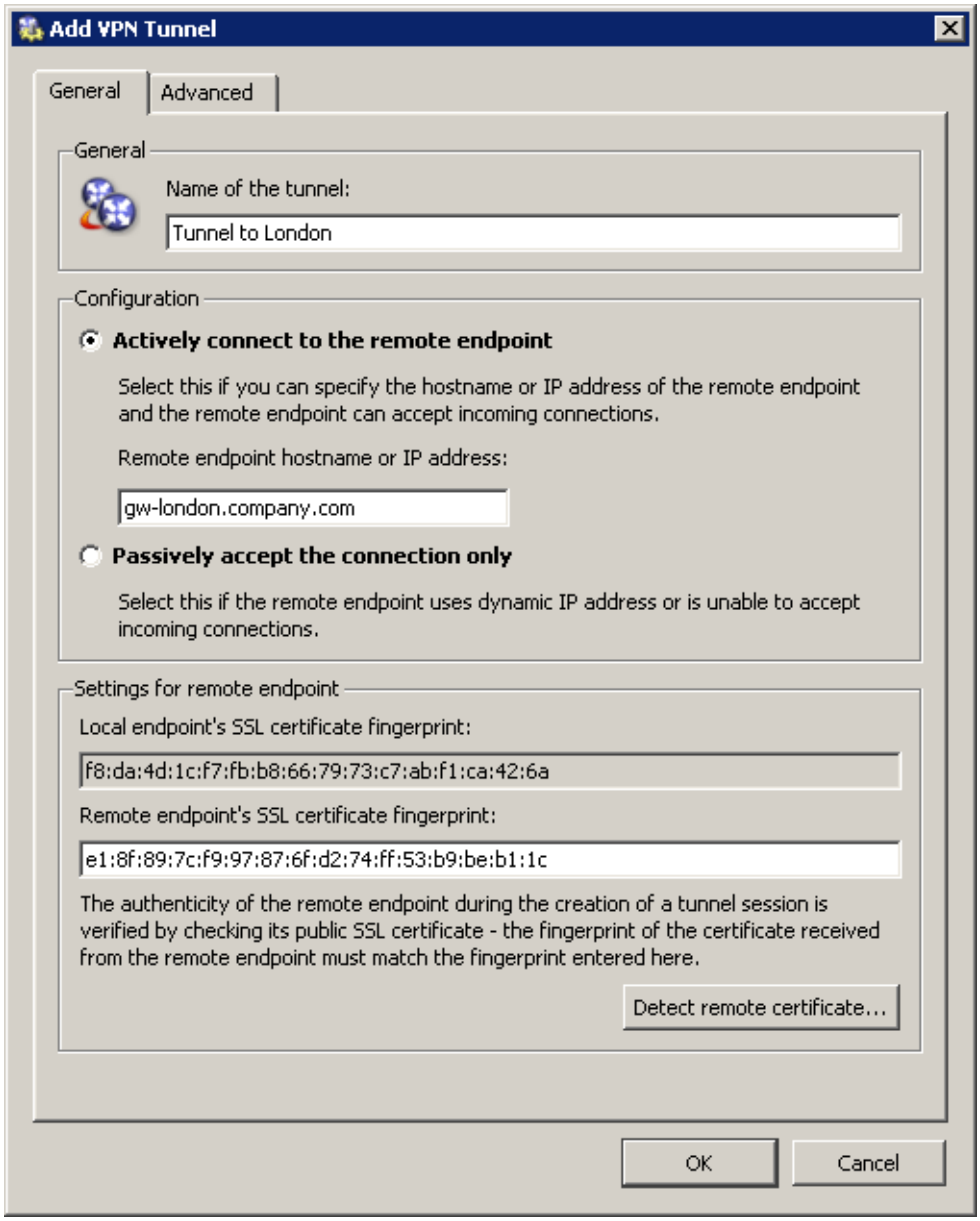

Add VPN Tunnel
General
Advanced
General
Name of the tunnel:
Tunnel to London
Configuration
Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
gw-london.company.com
Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept incoming connections.
Settings for remote endpoint
Local endpoint's SSL certificate fingerprint:
f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a
Remote endpoint's SSL certificate fingerprint:
e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.
Detect remote certificate...
OK
Cancel

Figure 21.62 The Paris filial office — definition of VPN tunnel for the London filial office

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *London's* local networks.

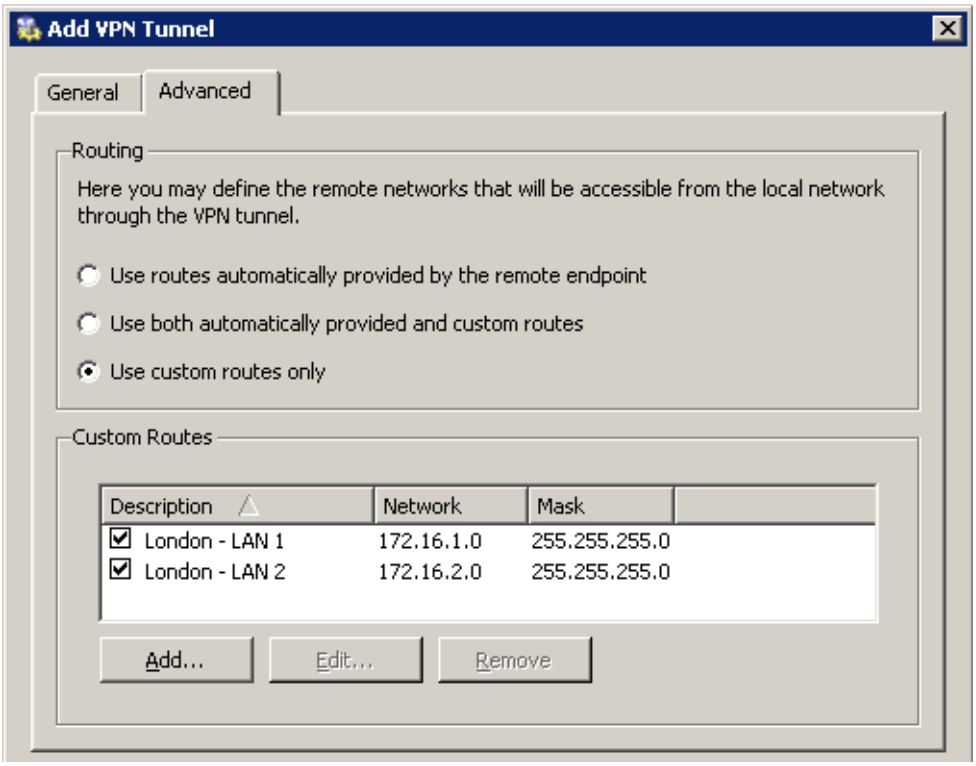


Figure 21.63 The Paris filial — routing configuration for the tunnel connected to the London branch office

Like in the previous step, check whether the tunnel has been established successfully, and check reachability of remote private networks (i.e. of local networks in the *London* filial).

7. Add the new VPN tunnels into the *Local Traffic* rule. It is also possible to remove the *Dial-In* interface and the *VPN clients* group from this rule (VPN clients are not allowed to connect to this branch office).

Name	Source	Destination	Service	Action	Translation
Local Traffic	LAN Firewall Tunnel to company headquarters Tunnel to London	LAN Firewall Tunnel to company hea Tunnel to London	Any	✓	
Firewall Traffic	Firewall	Internet	Any	✓	
Service Kerio VPN	Internet	Firewall	Kerio VPN	✓	

Figure 21.64 The Paris filial office — final traffic rules

VPN test

The VPN configuration has been completed by now. At this point, it is recommended to test reachability of the remote hosts in the other remote networks (at remote endpoints of individual tunnels).

For example, the `ping` or/and `tracert` operating system commands can be used for this testing.

Chapter 22

Kerio Clientless SSL-VPN

Kerio Clientless SSL-VPN (thereinafter "*SSL-VPN*") is a special interface used for secured remote access to shared items (files and folders) in the network protected by *WinRoute* via a web browser.

To a certain extent, the *SSL-VPN* interface is an alternative to *Kerio VPN Client* (see chapter 21). Its main benefit is that it enables an immediate access to a remote network from any location without any special application having been installed and any configuration having been performed (that's the reason for calling it *clientless*). The main disadvantage of this alternative is that network connections are not transparent. *SSL-VPN* is, in a manner, an alternative to the *My Network Places* system tool) — it does not enable access to web servers or other services in a—remote network.

SSL-VPN is suitable for an immediate access to shared files in remote networks in such environments where it is not possible or useful to use *Kerio VPN Client*.

22.1 Configuration of WinRoute's SSL-VPN

Usage of *SSL-VPN* is conditioned by membership of the *WinRoute* host in the corresponding domain (Windows NT or Active Directory). User accounts that will be used for connections to *SSL-VPN* must be authenticated at the domain (it is not possible to use local authentication). This implies that *SSL-VPN* cannot be used for accessing shared items in multiple domains or to items at hosts which are not members of any domain.

SSL-VPN configuration

The *SSL-VPN* interface can be enabled/disabled on the *Web Interface* → *SSL-VPN* in the *Configuration* → *Advanced Options* section.

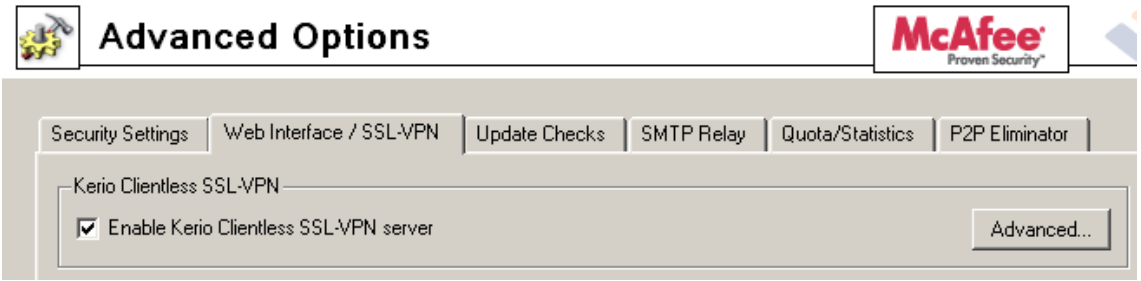


Figure 22.1 Configuration of the SSL-VPN interface

Click *Advanced* to open a dialog where port and SSL certificate for *SSL-VPN* can be set.

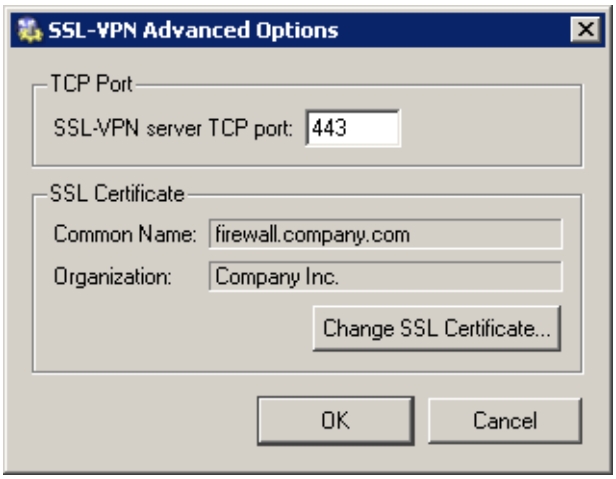


Figure 22.2 Setting of TCP port and SSL certificate for SSL-VPN

SSL-VPN's default port is port `443` (standard port of the *HTTPS* service).

Click *Change SSL Certificate* to create a new certificate for the *SSL-VPN* service or to import a certificate issued by a trustworthy certification authority. When created, the certificate is saved as `sslvpn.crt` and the corresponding private key as `sslvpn.key`. The process of creating/importing a certificate is identical as the one for *WinRoute's* interface or the VPN server, addressed in detail in chapter 9.1.

HINT: Certificates for particular server name issued by a trustworthy certification authority can also be used for the Web interface and the VPN server — it is not necessary to use three different certificates.

Allowing access from the Internet

Access to the *SSL-VPN* interface from the Internet must be allowed by defining a traffic rule allowing connection to the firewall's *HTTPS* service.

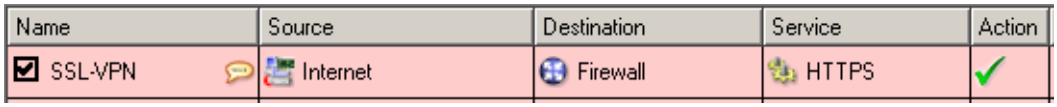


Figure 22.3 Traffic rule allowing connection to the SSL-VPN interface

Note: If the port for *SSL-VPN* interface is changed, it is also necessary to modify the *Service* item in this rule!

22.2 Usage of the SSL-VPN interface

For access to the interface, most of common graphical web browsers can be used (however, we recommend to use *Microsoft Internet Explorer* version 6.0 or *Firefox/Netscape/Mozilla/SeaMonkey* with the core version 1.3 and later). Specify URL in the browser in the

```
https://server/
```

format, where `server` represents the DNS name or IP address of the *WinRoute* host. If *SSL-VPN* uses another port than the default port for *HTTPS* (443), it is necessary to specify the used port in the URL, e.g.

```
https://server:12345/
```

Upon a connection to the server, the *SSL-VPN* interface's welcome page is displayed localized to the language set in the browser. If the language defined as preferred is not available, the English version will be used.

For access to the network by *SSL-VPN*, authentication to the particular domain at the login page by username and password is required. Any operations with shared files and folders are performed under the identity of the user currently logged in.

Figure 22.4 Clientless SSL-VPN — login dialog

Method of specification of the login name depends on the configuration of the particular user account in *WinRoute* (see chapter 13):

- If an account is defined in the local user database, the username must be specified without the domain (e.g. `jsmith`).

  Warning: Only accounts authenticated in *Active Directory* or *Windows NT* domain (*NT/Kerberos 5* authentication) can be used for access to the *SSL-VPN* interface. Ac-

counts authenticated only in *WinRoute* (*Internal user database* authentication) cannot be used to access *SSL-VPN*. For details on local user accounts, refer to chapter 13.2.

- If it is a mapped *Active Directory* domain which is set as primary (or if only one domain is mapped), it is possible to specify username either leaving out the domain (`jdolittle`) or with the domain (`jdolittle@company.com`).
- If it is a mapped *Active Directory* domain which is not set as primary, the domain must be included in the username specification (e.g. `sidneywashington@usoffice.company.com`).

Handling files and folders

The way the *SSL-VPN* interface is handled is similar to how the *My Network Places* system window is used.

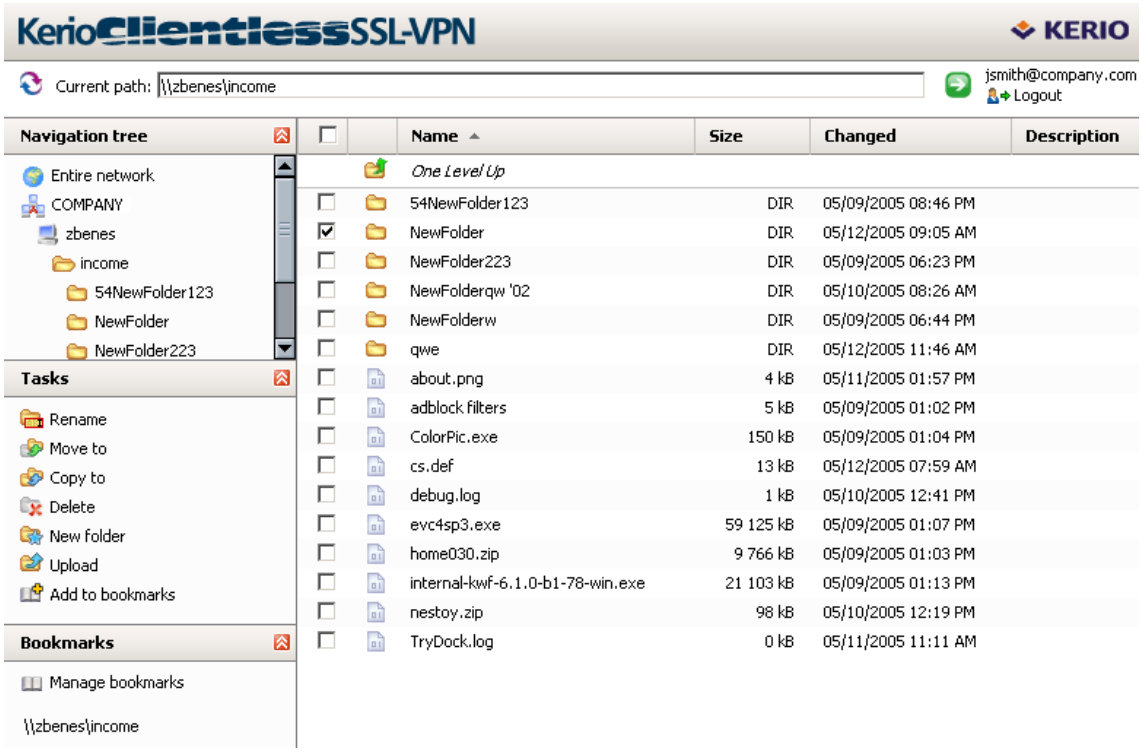


Figure 22.5 Clientless SSL-VPN — main page

At the top of the page, an entry is available, where location of the demanded shared item (so called *UNC path*) can be specified — for example:

```
\\server\folder\subfolder
```

All shared items in the domain can be browsed using a so called navigation tree on the left. The navigation tree is linked to the entry (this means that in the entry, the path associated with the selected item in the tree is displayed, and vice versa — if a path is entered in the line, a corresponding item is selected in the tree).

Right under the navigation tree, actions available for the specified location (i.e. for the selected item or folder) is provided. The basic functions provided by the *SSL-VPN* interface are download of a selected file to the local host (the host where the user's browser is running) and uploading a file from the local host to a selected location in the remote domain (the user must have write rights for the destination). Downloading or uploading of more than one file or of entire folders is not possible.

For files, any standard functions, such as copying, renaming, moving and removals, are still available. Files can be copied or moved within the frame of shared files in the particular domain.

In a selected location, empty folders can be created and deleted. It is not possible to move or copy folders.

Antivirus control

If at least one antivirus is enabled in *WinRoute* (see chapter 11), all files uploaded to remote hosts are automatically scanned for viruses. For connection speed reasons, files downloaded to local hosts from remote networks are not scanned by antiviruses (files downloaded from private networks are considered as trustworthy).

Bookmarks

For quick access to frequently used network items, so called bookmarks can be created. Bookmarks work on principles similar to the *Favorites* tool in *Windows* operating systems.

Bookmarks can be created for currently selected location (i.e. for the path displayed in the entry) and it is also possible to specify demanded UNC path by hand in the bookmark definition section. It is recommended to label by a short unique name — this will help you with the bookmarks maintenance, especially if more bookmarks are used. If the name is not specified, the bookmark will be listed in the list of bookmarks under the UNC path.

Chapter 23

Troubleshooting

This chapter provides several helpful tips for solving of problems which might arise during *WinRoute* deployment.

23.1 Detection of incorrect configuration of the default gateway

One of the most common problems ocurred in *WinRoute* implementation is incorrect configuration of default gateways in the operating system by the computer where *WinRoute* is installed. Therefore, *WinRoute* (since *6.2.0*) automatically detects configuration of default gateways in the system. If an incorrect configuration is detected (i.e. more than one default gateway is defined in the system), the following alert is displayed upon the next login to the *Administration Console*.

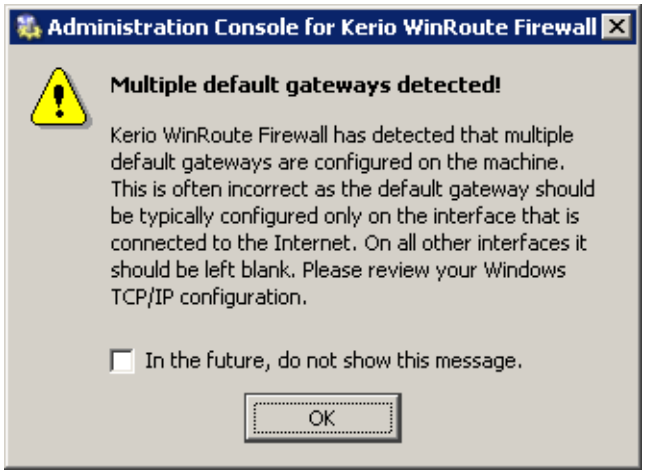

Administration Console for Kerio WinRoute Firewall
Multiple default gateways detected!
Kerio WinRoute Firewall has detected that multiple default gateways are configured on the machine. This is often incorrect as the default gateway should be typically configured only on the interface that is connected to the Internet. On all other interfaces it should be left blank. Please review your Windows TCP/IP configuration.
In the future, do not show this message.
OK

Figure 23.1 An alert pointing at incorrect configuration of the default gateway

In such a case, it is necessary to check TCP/IP configuration at all interfaces of the *WinRoute's* host. One of the indicators that may help you detect incorrect settings can be listing of the system routing table by using the `route print` command (the default gateway is displayed as a path to the destination network *0.0.0.0* with subnet mask *0.0.0.0*). The default gateway must be set only on the interface connected to the Internet (in accordance with information provided by the ISP). If any default gateway is set at other network interface(s), the configuration is wrong.

Once configuration of network interfaces is corrected, it is not necessary to restart the computer or *WinRoute Firewall Engine*. Simply login to the *Administration Console* again to make sure that the incorrect settings have been fixed (i.e. the alert is not displayed). Typically, traffic from the local network to the Internet starts working at this point.

A configuration example along with detailed instructions is provided in the *Kerio WinRoute Firewall — Step-by-Step* guide.

It is strongly recommended not to disable displaying of this alert — whenever configuration of network interfaces is changed, the problem may occur again!

Note: In very special cases, existence of more default gateways (with different metrics) may be desired. If you are sure that your configuration is correct and if all traffic between the local network and the Internet is working smoothly, you can disable displaying of the alert.

23.2 Configuration Backup and Transfer

Configuration files

All *WinRoute* configuration data is stored in the following files under the same directory where *WinRoute* is installed

(the typical path is `C:\Program Files\Kerio\WinRoute Firewall`).

The following files are included:

winroute.cfg
: Chief configuration file

UserDB.cfg
: Information about groups and user accounts.

host.cfg
: Preferences for backs-up of configuration, user accounts data, DHCP server database, etc.

logs.cfg
: Log configurations

Note: The data in these files are saved in XML format so that it can be easily modified by an advanced user or generated automatically using another application.

Files in the following directories are also considered as configuration data:

dbSSL
: An automatically generated SSL certificate generated for traffic between the *WinRoute Firewall Engine* and the *Administration Console*.

For details on traffic between the *WinRoute Firewall Engine* and the *Administration Console*, refer to *Kerio Administration Console — Help* (`http://www.kerio.com/kwf-manual`).

sslcert
SSL certificates for all components using SSL for traffic encryption (i.e. the web interface, VPN server and the *Clientless SSL-VPN* interface).

license
If *WinRoute* has already been registered, the `license` folder includes a license key file (including registered trial versions). If *WinRoute* has not been registered yet, the `license` folder is empty.

Status files

In addition, *WinRoute* generates other files and directories where certain status information is saved:

Files:

Cache.CFS
Current *ISS OrangeWeb Filter's* cache data (see chapter 10.4).

dnscache.cfg
DNS files stored in *DNS forwarder's* cache (see chapter 5.3).

leases.cfg
IP addresses assigned by the DHCP server.
This file keeps all information available on the *Leases* tab of the *Configuration* → *DHCP server* section (refer to chapter 5.4).

ofclient.cfg
Current *ISS OrangeWeb Filter* configuration data (see chapter 10.4).
This file is generated automatically in accordance with *ISS OrangeWeb Filter* settings made in the main configuration file (`winroute.cfg`) and it is refreshed upon any change of these settings.

stats.cfg
Interface statistics (see chapter 18.1) and user statistics (see chapter 18.2) data.

vpnleases.cfg
IP addresses assigned to VPN clients (see chapter 21.2).

Directories:

logs
: The `logs` directory stores all *WinRoute* logs (see chapter 20).

star
: The `star` directory includes a complete database for statistics of the *WinRoute's* web interface.

Handling configuration files

Warning: We recommend that *WinRoute Firewall Engine* be stopped prior to any manipulation with the configuration files (backups, recoveries, etc.)! Information contained within these files is loaded and saved only upon starting or stopping the MailServer. All changes to the configuration performed while the *Engine* is running are only stored in memory. All modifications done during *Engine* performance will be overwritten by the configuration in the system memory when the *Engine* is stopped.

Configuration backup recovery

Configuration can be backed-up by copying all the previously described configuration and/or status files.

To recover configuration through backed-up data (typically this need may arise when *WinRoute* is installed to a new workstation or when the operating system is being reinstalled), follow these steps:

1. Perform *WinRoute* installation on a required machine (refer to chapter 2.3).
2. Stop *WinRoute Firewall Engine*.
3. Into the *WinRoute* directory

   (typically the path `C:\Program Files\Kerio\WinRoute Firewall`)

   copy the back-up files `host.cfg`, `logs.cfg`, `UserDB.cfg` and `winroute.cfg`
4. Copy license and SSL certificate subdirectories (`license`, `sslcert` and `dbSSL`).
5. Copy status files and directories (files `Cache.CFS`, `dnscache.cfg`, `leases.cfg`, `ofclient.cfg`, `stats.cfg`, `vpnclient.cfg` and directories `logs` and `star`).
6. Run *WinRoute Firewall Engine*.

   At this stage, *WinRoute* detects the required configuration file. Within this process, unknown network interfaces (ones which are not defined in the `winroute.cfg` configuration file) will be detected in the system. Each network interface includes

a unique (randomly generated) identifier in the operating system. It is almost not possible that two identifiers were identical.

To avoid setting up new interfaces and changing traffic rules, you can assign new identifiers to original interfaces in the `winroute.cfg` configuration file.

7. Stop *WinRoute Firewall Engine*.

8. Use a plaintext editor (e.g. *Notepad*) to open the `winroute.cfg` configuration file. Go to the following section:

   ```
   <list name="Interfaces">
   ```

   Scan this section for the original adapter. Find an identifier for a new interface in the new adapter's log and copy it to the original adapter. Remove the new interface's log.

   Example: Name of the local network interface is *LAN*. This network connection is labeled as *Local Area Connection* in the new operating system. Now, the following data can be found in the `Interfaces` section (only the essential parts are listed):

   ```
   <listitem>
     <variable name="Id">
       \DEVICE\{7AC918EE-3B85-5A0E-8819-CBA57D4E11C7}
     </variable>
     <variable name="Name">LAN</variable>
     ...
   </listitem>
   <listitem>
     <variable name="Id">
       \DEVICE\{6BF377FB-3B85-4180-95E1-EAD57D5A60A1}
     </variable>
     <variable name="Name">Local Area Connection</variable>
     ...
   </listitem>
   ```

   Copy the `Local Area Connection` interface's identifier into the `LAN` interface. Remove the data for `Local Area Connection` (a relevant `listitem` section).

   When all these changes are performed, the data in the configuration file relating to interface connected to the local network will be as follows:

   ```
   <listitem>
     <variable name="Id">
       \DEVICE\{6BF377FB-3B85-4180-95E1-EAD57D5A60A1}
     </variable>
   ```

```
    <variable name="Name">LAN</variable>
    ...
  </listitem>
```

9. Save the `winroute.cfg` file and run *WinRoute Firewall Engine*.

Now, the *WinRoute* configuration is identical with the original *WinRoute* configuration on the prior operating system.

Note: The method described above includes a complete "clone" of *WinRoute* on a new host. Some of the steps are optional — for example, if you do not wish to keep the current statistics, do not copy the `star` subdirectory.

23.3 Automatic user authentication using NTLM

WinRoute supports automatic user authentication by the NTLM method (authentication from Web browsers). Users once authenticated for the domain are not asked for username and password.

This chapter provides detailed description on conditions and configuration settings for correct functioning of NTLM.

General conditions

The following conditions are applied to this authentication method:

1. *WinRoute Firewall Engine* is running as a service or it is running under a user account with administrator rights to the *WinRoute* host.

2. The server (i.e. the *WinRoute* host) belongs to a corresponding Windows NT or Kerberos 5 (Windows 2000/2003) domain.

3. Client host belongs to the domain.

4. User at the client host is required to authenticate to this domain (i.e. local user accounts cannot be used for this purpose).

5. The *NT domain / Kerberos 5* authentication method (see chapter 13.1) must be set for the corresponding user account under *WinRoute*. NTLM cannot be used for authentication in the internal database.

WinRoute Configuration

NTLM authentication of users from web browsers must be enabled in *Users* → *Authentication Options*. User authentication should be required when attempting to access web pages, otherwise enabling NTLM authentication is meaningless.

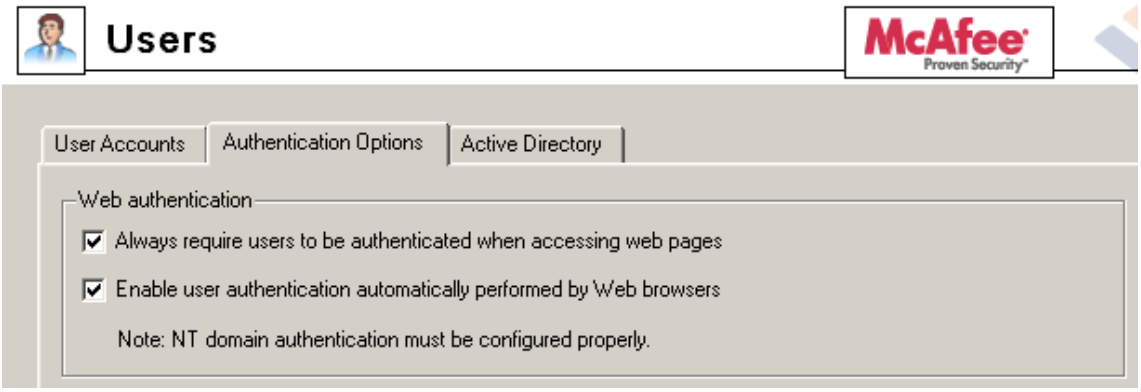


Figure 23.2 NTLM — user authentication options

User authentication in the corresponding NT domain must be enabled.

- *For local user accounts* (including accounts imported manually or automatically from the domain) — at the bottom of the *Authentication Options* tab, NT authentication must be enabled and the corresponding NT domain must be set (e.g. `COMPANY`).

Figure 23.3 Setting of NT authentication for local user accounts

- *For mapped Active Directory domain* — the corresponding NT domain must be set in the particular domain's configuration on the *Active Directory* tab (for details, refer to chapter 13.4).

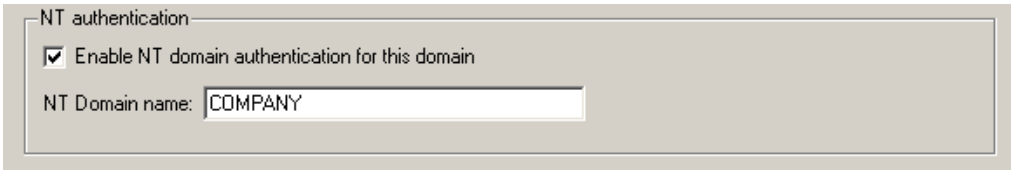


Figure 23.4 Setting of NTLM authentication for a mapped Active Directory domain

The configuration of the *WinRoute's* web interface must include a valid DNS name of the server on which *WinRoute* is running (for details, see chapter 9.1).

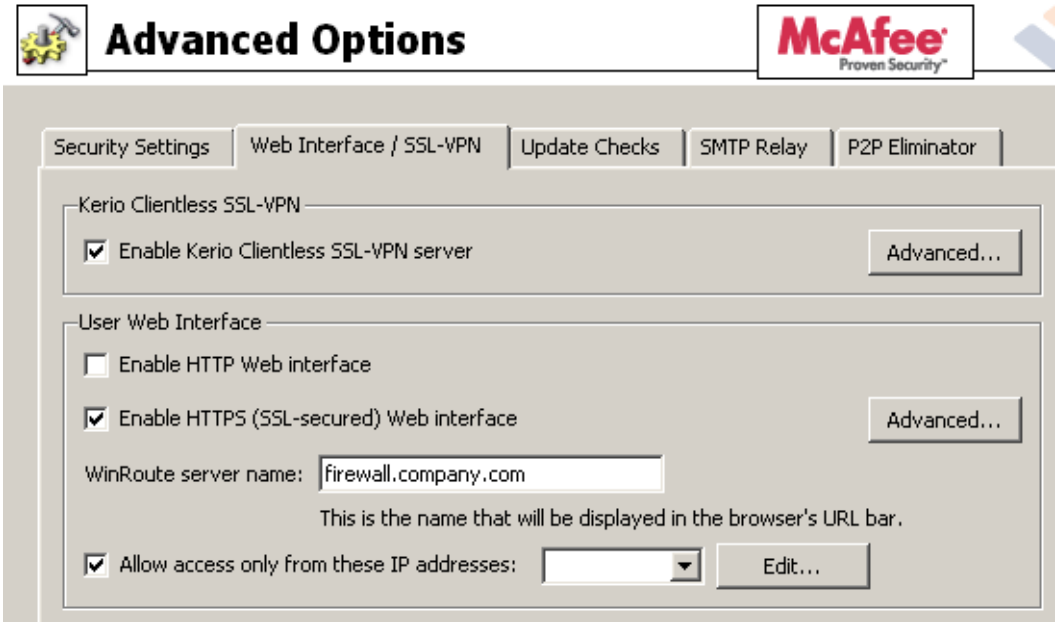


Figure 23.5 Configuration of WinRoute's Web Interface

Web browsers

For proper functioning of NTLM, a browser must be used that supports this method. By now, the following browsers are suitable:

- *Microsoft Internet Explorer* version *5.01* or later
- *Firefox, Netscape, Mozilla or SeaMonkey* with the core version *Mozilla 1.3* or later

NTLM authentication process

NTLM authentication process differs depending on a browser used.

Microsoft Internet Explorer

NTLM authentication is performed without user's interaction.
The login dialog is displayed only if NTLM authentication fails (e.g. when user account for user authenticated at the client host does not exist in *WinRoute*).
Warning: One reason of a NTLM authentication failure can be invalid login username or password saved in the *Password Manager* in *Windows* operating systems (*Control Panels* → *User Accounts* → *Advanced* → *Password Manager*) applying to the corresponding server (i.e. the *WinRoute* host). In such a case, *Microsoft Internet*

Explorer sends saved login data instead of NTLM authentication of the user currently logged in. Should any problems regarding NTLM authentication arise, it is recommended to remove all usernames/passwords for the server where *WinRoute* is installed from the *Password Manager*.

Firefox/Netscape/Mozilla/SeaMonkey
The browser displays the login dialog. For security reasons, automatic user authentication is not used by default in the browser. This behaviour of the browser can be changed by modification of configuration parameters — see below.
If authentication fails and direct connection is applied, the firewall's login page is opened automatically (refer to chapter 9.2). The login dialog is displayed if proxy server is used.

Note: If NTLM authentication fails by any reason, details are recorded in the *error* log (see chapter 20.8).

Firefox/Netscape/Mozilla/SeaMonkey configuration

Configuration can be changed to enable automatic NTLM authentication — leaving out the login dialog. To set this, follow this guidance:

1. Insert `about:config` in the browser's address bar. The list of configuration parameters is displayed.

2. Set corresponding configuration parameter(s) using the following instructions:

   - For direct connection (proxy server is not set in the browser):

     Look up the `network.automatic-ntlm-auth.trusted-uris` parameter. Use the *WinRoute* host's name as a value for this parameter (e.g. `server` or `server.company.com`). This name must match the server name set under *Configuration* → *Advanced Options* → *Web Interface* (see chapter 9.1).

     Note: It is not possible to use IP address as a value in this parameter!

   - If *WinRoute* proxy server is used:

     Look up the `network.automatic-ntlm-auth.allow-proxies` parameter and set its value to `true`.

   Configuration changes are applied right away, i.e. it is not necessary to restart the browser.

23.4 Partial Retirement of Protocol Inspector

Under certain circumstances, appliance of a protocol inspector to a particular communication might be undesirable. To disable specific protocol inspection, define corresponding source and destination IP addresses and a traffic rule for this service that will define explicitly that no protocol inspector will be used.

Example: A banking application (client) communicates with the bank's server through its proper protocol which uses TCP protocol at the port 2000. Supposing the banking application is run on a host with IP address `192.168.1.15` and it connects to the server `server.bank.com`.

This port is used by the *Cisco SCCP* protocol. The protocol inspector of the *SCCP* would be applied to the traffic of the banking client under normal circumstances. However, this might affect functionality of the application or endanger its security.

A special traffic rule, as follows, will be defined for all traffic of the banking application:

1. In the *Configuration* → *Definitions* → *Services* section, define a service called *Internet Banking*: this service will use TCP protocol at the port 2000 and no protocol inspector is used by this communication.

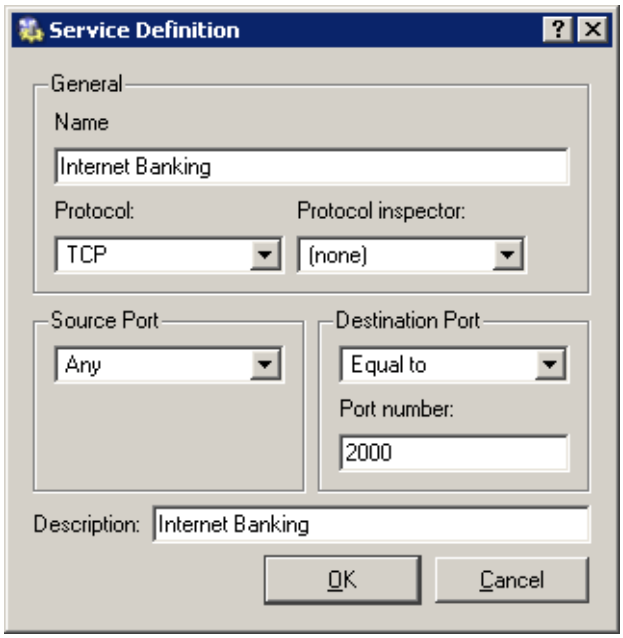


Figure 23.6 Service definition without inspector protocol

2. In the *Configuration* → *Traffic Policy* section, create a rule which will permit this service traffic between the local network and the bank's server. Specify that no protocol inspector will be applied.

Figure 23.7 This traffic rule allows accessing service without protocol inspection

Note: In the default configuration of the *Traffic rules* section, the *Protocol inspector* column is hidden. To show it, modify settings through the *Modify columns* dialog (see chapter 3.2).

Warning: To disable a protocol inspector, it is not sufficient to define a service that would not use the inspector! Protocol inspectors are applied to all traffic performed by corresponding protocols by default. To disable a protocol inspector, special traffic rules must be defined.

23.5 User accounts and groups in traffic rules

In traffic rules, source/destination can be specified also by user accounts or/and user groups. In traffic policy, each user account represents IP address of the host from which user is connected. This means that the rule is applied to users authenticated at the firewall only (when the user logs out, the rule is not effective any longer). This chapter is focused on various issues relating to use of user accounts in traffic rules as well as hints for their solution.

Note: For detailed information on traffic rules definition, refer to chapter 6.3.

How to enable certain users to access the Internet

How to enable access to the Internet for specific users only? Assuming that this problem applies to a private local network and Internet connection is performed through NAT, simply specify these users in the *Source* item in the NAT rule.

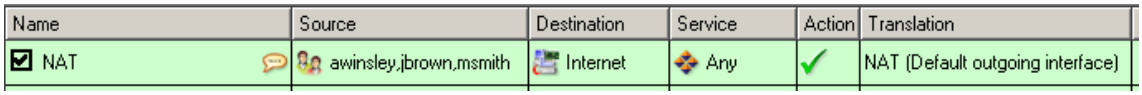


Figure 23.8 This traffic rule allows only selected users to connect to the Internet

Such a rule enables the specified users to connect to the Internet (if authenticated). However, these users must open the *WinRoute* interface's login page manually and authenticate (for details, see chapter 8.1).

However, with such a rule defined, all methods of automatic authentication will be ineffective (i.e. redirecting to the login page, NTLM authentication as well as automatic authentication from defined hosts). The reason is that the automatic authentication (or redirection to the login page) is not invoked unless connection to the Internet is being established (for license counting reasons — see chapter 4.6). However, this NAT rule blocks any connection unless the user is authenticated.

Enabling automatic authentication

The automatic user authentication issue can be solved easily as follows:

- Add a rule allowing an unlimited access to the *HTTP* service before the NAT rule.

Figure 23.9 These traffic rules enable automatic redirection to the login page

- In URL rules (see chapter 10.2), allow specific users to access any Web site and deny any access to other users.

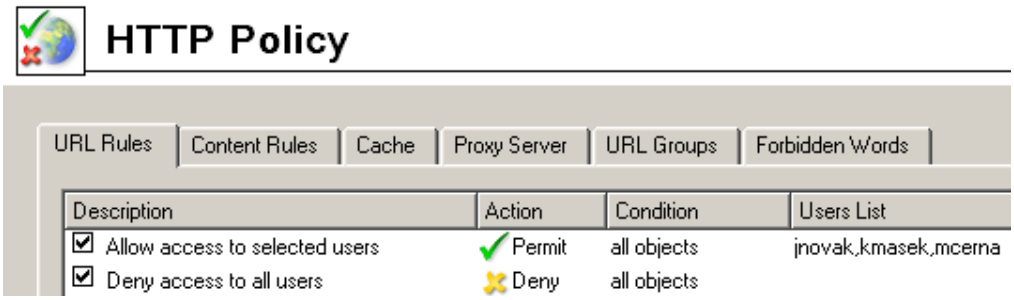


Figure 23.10 These URL rules enable specified users to access any Web site

User not authenticated yet who attempts to open a Web site will be automatically redirected to the authentication page (or authenticated by NTLM, or logged in from the corresponding host). After a successful authentication, users specified in the *NAT* rule (see figure 23.9) will be allowed to access also other Internet services. As well as users not specified in the rules, unauthenticated users will be disallowed to access any Web site or/and other Internet services.

Note: In this example, it is assumed that client hosts use the *WinRoute DNS Forwarder* or local DNS server (traffic must be allowed for the DNS server). If client stations used a DNS server in the Internet (this configuration is not recommended!), it would be necessary to include the *DNS* service in the rule which allows unlimited Internet access.

23.6 FTP on WinRoute's proxy server

Proxy server in *WinRoute*, version *6.0.2* and later (see chapter 5.5), supports FTP. When using this method of accessing FTP servers, it is necessary to keep in mind specific issues regarding usage of the proxy technology and parameters of *WinRoute's* proxy server.

1. It is necessary that the FTP client allows configuration of the proxy server. This condition is met for example by web browsers (*Internet Explorer*, *Firefox/Netscape/Mozilla/SeaMonkey*, *Opera*, etc.), *Total Commander* (originally *Windows Commander*), *CuteFTP*, etc.

   Terminal FTP clients (such as the `ftp` command in *Windows* or *Linux*) do not allow configuration of the proxy server. For this reason, they cannot be used for our purposes.

2. To connect to FTP servers, the proxy server uses the passive FTP mode. If FTP server is protected by a firewall which does not support FTP (this is not a problem of *WinRoute*), it is not possible to use proxy to connect to the server.

3. Setting of FTP mode in the client is irrelevant for usage of the proxy server. Only one network connection used by the FTP protocol is always established between a client and the proxy server.

Note: It is recommended to use FTP over proxy server only in cases where it is not possible to connect directly to the Internet (see chapter 5.5).

Example of a client configuration: web browser

Web browsers allow to set the proxy server either globally or for individual protocols. In our example, configuration of *Microsoft Internet Explorer 6.0* focused (configuration of any other browsers is almost identical).

1. In the browser's main menu, select *Tools* → *Internet Options*, open the *Connections* tab and click on the *LAN Settings* option.

2. Enable the *Use a proxy server for your LAN* option and enter the IP address and port of the proxy server. IP address of the proxy server is the address of the *WinRoute's* host interface which is connected to the local network; the default port of the proxy

server is 3128 (for details, refer to chapter 5.5). It is also recommended to enable the *Bypass proxy server for local addresses* option — using proxy server for local addresses would slow down traffic and overburden *WinRoute*.

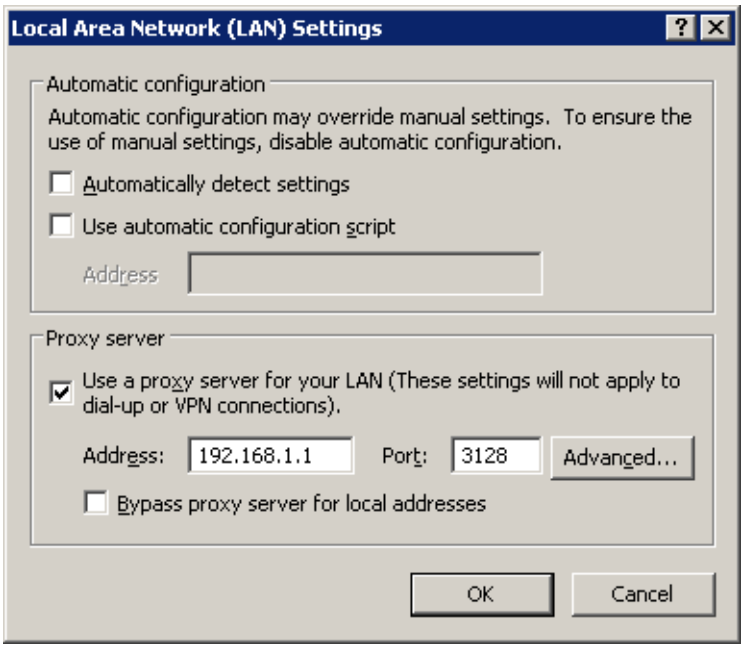

Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 192.168.1.1
Port: 3128
Advanced...
Bypass proxy server for local addresses
OK
Cancel

Figure 23.11 Configuring proxy server in Microsoft Internet Explorer

HINT: To configure web browsers, you can use a configuration script or the automatic detection of configuration. For details, see chapter 5.5.

Note: Web browsers used as FTP clients enable only to download files. Uploads to FTP server via web browsers are not supported.

Example of a client configuration: Total Commander

Total Commander allows either single connections to FTP server (by the *Net* → *FTP - New Connection* option available in the main menu) or creating a bookmark for repeated connections (*Net* → *FTP - Connect*). The proxy server must be configured individually for each FTP connection (or for each bookmark).

1. In the *FTP: connection details* dialog, enable the *Use firewall (proxy server)* option and click *Change*.

2. In the *Firewall settings* dialog box, select *HTTP Proxy with FTP support*. In the *Host name* textbox, enter the proxy server's IP address and port (separated by a colon, e.g. `192.168.1.1:3128`). The *User name* and *Password* entries are optional (*WinRoute* does not use this information).

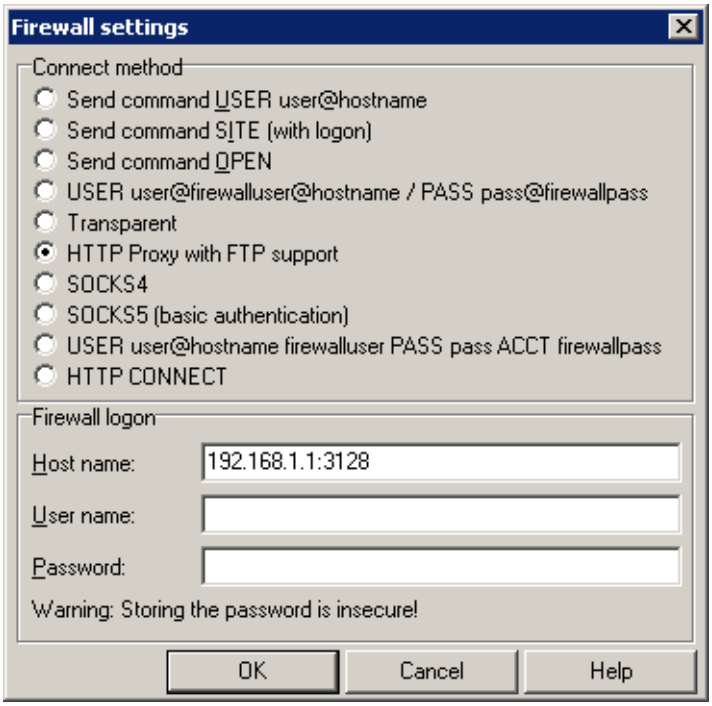


Figure 23.12 Setting proxy server for FTP in Total Commander

HINT: The defined proxy server is indexed and saved to the list of proxy servers automatically. Later, whenever you are creating other FTP connections, you can simply select a corresponding proxy server in the list.

Chapter 24

Network Load Balancing

Certain versions of the *Microsoft Windows* operating system allow creation of so called cluster — a group of hosts which behaves as a single virtual server. Clients' requests to the virtual server are distributed to individual computers within the cluster. This technology is called *Network Load Balancing* (called *NLB* in the further text). If *WinRoute* and *NLB* are used, a particular local network can be connected to the Internet by several independent lines. Network communication will be distributed to these lines in accordance with the corresponding settings (evenly or in dependence on speed of individual lines, etc.).

The cluster technology provides several benefits, such as increasing of permeability, response speed and reliability of the Internet connection.

24.1 Basic Information and System Requirements

Creating of a *NLB* cluster are supported by following operating systems:

- *Windows 2000 Advanced Server* or *Datacenter Server*
- *Windows Server 2003 Enterprise Edition* or *Datacenter Edition*

To make functionality of the cluster as reliable as possible, it is necessary that the same operating system is installed at all servers participating.

WinRoute license for a corresponding number of users is needed for each server participating in the cluster (for details, see chapter 4.6).

Note: The listed versions of the operating systems allow creating of two cluster types: server clusters and Network Load Balancing cluster. These types cannot be combined.

24.2 Network Configuration

The example describes a cluster configuration where traffic between a local network and the Internet is divided to two Internet connections (refer to figure 24.1).

Each server needs two network interfaces: one for connection to the local network (usually, the *Ethernet* adapter is used) and another for connection to the Internet (e.g. *Ethernet* or *WiFi*). Various types of Internet connections can be used, however, these connections should be permanent. It is strongly recommended not to use dialed connections!

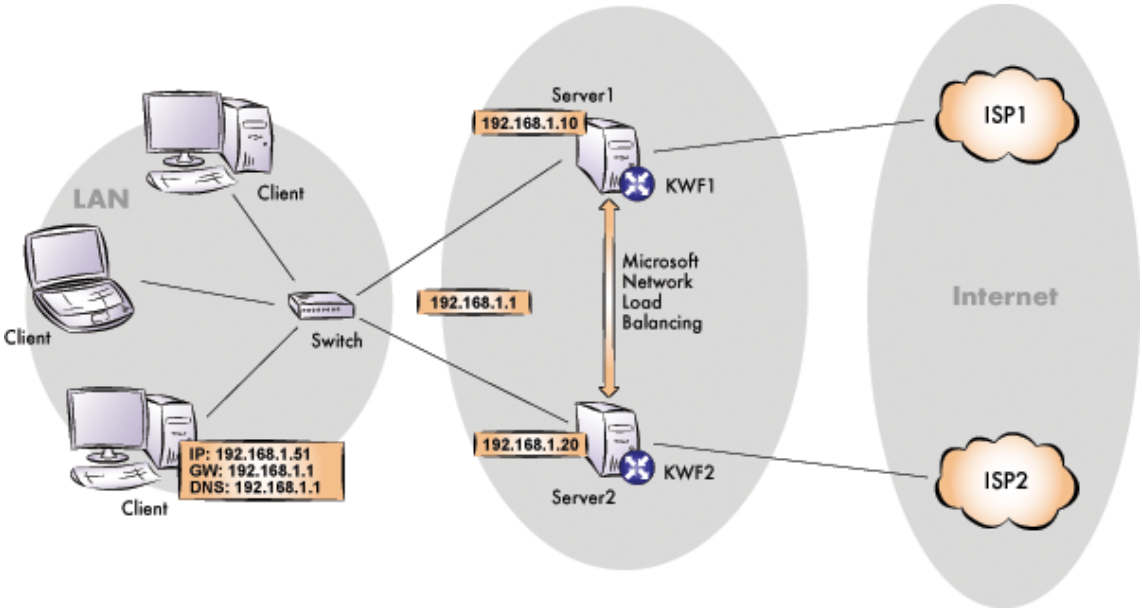


Figure 24.1 Network configuration for Network Load Balancing

1. Three IP addresses must be reserved when assigning IP addresses in the local network: two for servers and one for the cluster (i.e. for the virtual server). In this example, IP addresses `192.168.1.10` and `192.168.1.20` are assigned to the servers. The IP address `192.168.1.1` will be assigned to the cluster.

2. Both servers will be connected to the local network (if the configuration is more complicated, it is desirable to connect both servers to one switch). No special real interconnection of the servers is required.

   It is necessary to check functionality of both Internet connections.

3. Install *WinRoute* on both servers. Configuration of both servers should match (traffic rules should allow network communication between a particular server and the local network in both directions with no restrictions).

   Warning: The *DNS*, *DHCP* and *WINS* services for the local network must be run at a separate server (i.e. a server which does not belong to the cluster). If these services were located at servers within the cluster, their databases would not be consistent and the services would not work properly.

4. Test functionality of *WinRoute* at both servers (at any computer in the local network, set a default gateway for both servers and test availability of any computer through the Internet).

5. Set *NLB* parameters for each server (refer to chapter 24.3).

6. Set `192.168.1.1` (IP address of the cluster) as the IP address at default gateway for computers in the local network and, again, test availability of computers through the Internet.

   HINT: If logging of corresponding connections is enabled (at both servers) in the *WinRoute's* traffic rule for access to the Internet from the local network (see chapter 6.3), it is possible to use the *Filter* log to view how queries from a particular computer are distributed between both Internet connections.

24.3 Configuration of the servers in the cluster

NLB configuration for Server1

1. Select a connection to the local network and open a dialog where settings for this connection can be defined.

   In the *General* tab, enable the *Network Load Balancing* component..

2. In the advanced configuration of the TCP/IP of the network interface connected to the local network, add the cluster's IP address (`192.168.1.1`).

3. Open the dialog where properties of the *Network Load Balancing* component can be set.

   In the *Cluster Parameters* tab, set the IP address of the virtual server (`192.168.1.1`) with a corresponding network mask and its full DNS name.

   In the *Cluster operation mode* section, it is recommended to select the *Multicast* option. This will enable full traffic between individual servers in the cluster. This is important especially for the cluster administration (if the *Unicast* option was used, it would be inevitable to administer the cluster from a computer which is not included in the cluster).

4. In the *Host Parameters* tab, set priority of the server (the whole number 1 stands for the highest priority). Priority is also used as a unique identifier of the server for the cluster. It is also necessary to specify the server's IP address (identical with the primary address of a corresponding network interface.

   Note: In the *Port Rules* tab, specific rules for maintenance of the *TCP* and *UDP* traffic can be set. Only one rule is defined by default that determines that any traffic performed by these protocols will be equally distributed between all servers in the cluster.

HINT: Under *Windows Server 2003*, a wizard can be used to create the cluster (this wizard is included in the *Network Load Balancing Administration* tool).

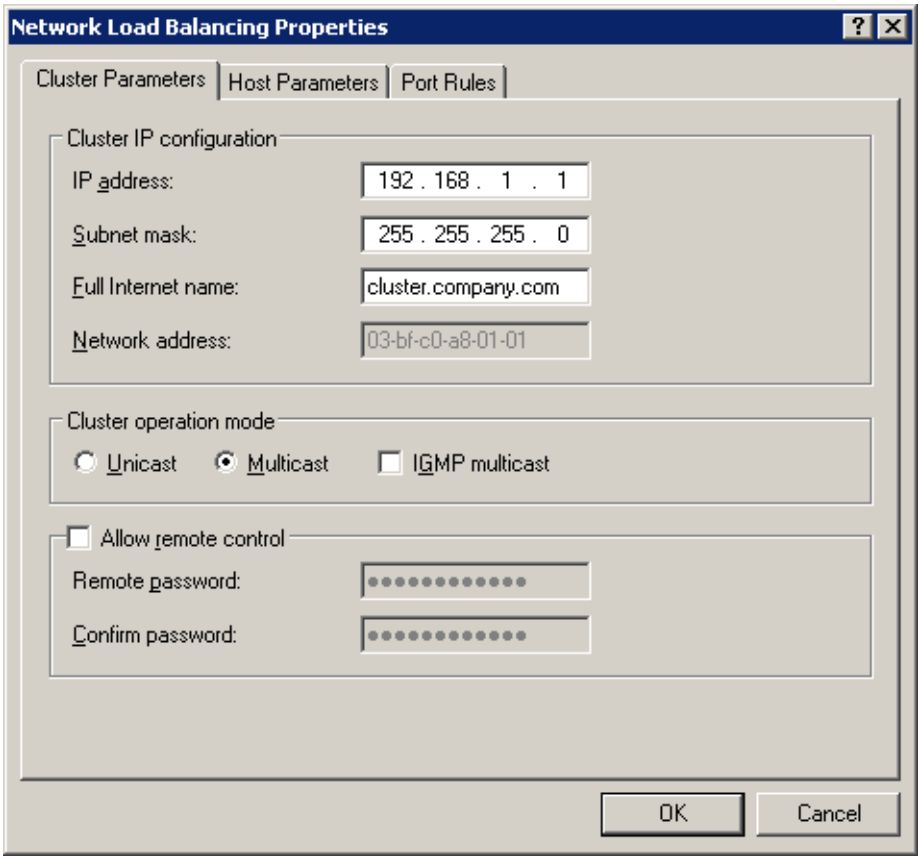


Figure 24.2 Server 1 — cluster parameters

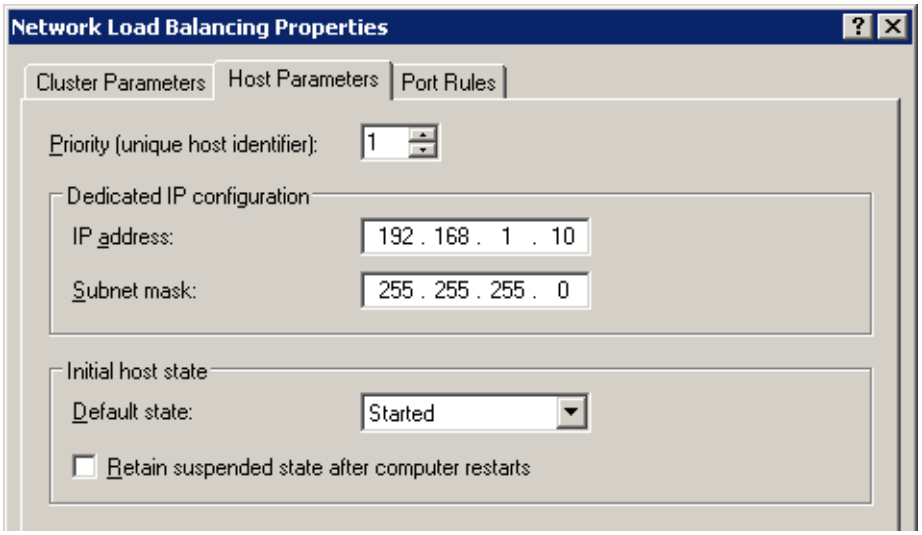


Figure 24.3 Server 1 — host parameters

NLB configuration for Server2

The configuration is almost the same in the case of `Server1`. However, IP address of the server is different (`192.168.1.20`) and it is also necessary to select different priority for the server (e.g. 2).

Note: The problem of cluster settings for load balancing is too wide and complicated to be described in this manual. Detailed information can be found at *Microsoft's* technical support Web site:

- Windows 2003: `http://support.microsoft.com/kb/323437/EN-US/`
- Windows 2000: `http://support.microsoft.com/kb/303608/EN-US/`

Chapter 25

Technical support

Free email and telephone technical support is provided for *Kerio WinRoute Firewall*. For contacts, see the end of this chapter. Our technical support staff is ready to help you with any problem you might have.

You can also solve many problems alone (and sometimes even faster). Before you contact our technical support, please take the following steps:

- Try to look up the answer in this manual. Individual chapters describe features and parameters of *WinRoute* components in detail.
- If you have not found answers here, try to find it in the *Technical Support* section of the Kerio Technologies website.

If you have not find answers to all your questions and you still intend to contact our technical support, read through the following section which will provide you with a few guidelines.

25.1 Essential Information

To send a request to our technical support, use the contact form at `http://support.kerio.com/`.

To be able to help you solve your problems the best and in the shortest possible time our technical support will require your configuration data and as clear information on your problem as possible. Please specify at least the following information:

Description

Clearly describe your problem. Provide as much information on the problem as possible (i.e. whether the issue arose after you had installed a new product version, after an upgrade, etc.).

Informational File

You can use the *Administration Console* to create a text file including your *WinRoute* configuration data. Take the following steps to generate the file:

- Run *WinRoute Firewall Engine* and connect to it through the *Administration Console*.
- If you use dial-up, connect to the Internet.
- In the *Administration Console* use the *Ctrl+S* keys.

The text file will be stored in the home directory of the logged user.

(e.g. `C:\Documents and Settings\Administrator`)

as `kerio_support_info.txt`.

Note: The `kerio_support_info.txt` is generated by the *Administration Console*. This implies that in case you connect to the administration remotely, this file will be stored on the computer from which you connect to the *WinRoute* administration (not on the computer/server where the *WinRoute Firewall Engine* is running).

Error Log Files

In the directory where *WinRoute* is installed

(typically the path `C:\Program Files\Kerio\WinRoute Firewall`)

the `logs` subdirectory is created. This directory includes the `error.log` and `warning.log` files. Attach these two files to your email to our technical support.

License type and license number

Please specify whether you have purchased any *WinRoute* license or if you use the trial version. Requirements of owners of valid licenses are always preferred.

25.2 Tested in Beta version

As to increase quality of our products, *Kerio Technologies* releases essential versions of our products as so called beta versions. Beta versions are product versions which include all projected new features, however, these functions and the product itself are still under development. Volunteers can test these versions and provide us with feedback to help us improve the product and fix bugs.

The feedback from beta testers is essential for the product's development. Therefore, *WinRoute* beta versions include extensions and modules helping testers communicate smoothly with *Kerio Technologies*.

For details on beta versions and their testing, refer to the http://www.kerio.com/beta web page.

25.3 Contacts

Kerio Technologies can be contacted at the following addresses:

USA

Kerio Technologies Inc.

2350 Mission College Blvd., Suite 400

Santa Clara, CA 95054

Phone: +1 408 496 4500

http://www.kerio.com/

Contact form: http://support.kerio.com/

United Kingdom

Kerio Technologies UK Ltd.

Enterprise House

Vision Park

Cambridge, CB4 9ZR

Histon

Tel.: +44 1223 202 130

http://www.kerio.co.uk/

Contact form: http://support.kerio.co.uk/

Czech Republic

Kerio Technologies s. r. o.

Anglicke nabrezi 1/2434

301 49 PLZEN

Phone: +420 377 338 902

http://www.kerio.com/

Contact form: http://support.kerio.cz/

Appendix A

Legal Presumption

Microsoft®, Windows®, Windows NT®, Internet Explorer® and Active Directory® are registered trademarks of Microsoft Corporation.

Mac OS® and Safari™ are registered trademarks or trademarks of Apple Computer, Inc.

Linux® is registered trademark of Linus Torvalds.

Mozilla® and Firefox® are registered trademarks of Mozilla Foundation.

Kerberos™ is trademark of Massachusetts Institute of Technology (MIT).

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.

Appendix B

Used open-source libraries

Kerio WinRoute Firewall contains the following open-source libraries:

IBPP

Copyright ©2000-2006 T.I.P. Group S.A. and the IBPP Team
Homepage: http://www.ibpp.org/
License agreement:
Permission is hereby granted, free of charge, to any person or organization ("You") obtaining a copy of this software and associated documentation files covered by this license (the "Software") to use the Software as part of another work; to modify it for that purpose; to publish or distribute it, modified or not, for that same purpose; to permit persons to whom the other work using the Software is furnished to do so; subject to the following conditions: the above copyright notice and this complete and unmodified permission notice shall be included in all copies or substantial portions of the Software; You will not misrepresent modified versions of the Software as being the original.
The Software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use of other dealings in the Software.

libiconv

Copyright ©1999-2003 Free Software Foundation, Inc.
Author: Bruno Haible
Homepage: http://www.gnu.org/software/libiconv/
The *libiconv* library is distributed and licensed as LGPL.
WinRoute includes a customized version of this library. Complete source codes of the customized version of *libiconv* library are available at:

http://download.kerio.com/dwn/iconv-patches

OpenSSL

This product contains software developed by *OpenSSL Project* designed for *OpenSSL Toolkit* (http://www.openssl.org/).

Prototype

Copyright ©2005 Sam Stephenson.
Homepage: http://prototype.conio.net/

zlib

Copyright ©1995-2005 Jean-Loup Gailly and Mark Adler.
Homepage: http://www.gzip.org/zlib/

Glossary of terms

ActiveX

This Microsoft's proprietary technology is used for creation of dynamic objects for Web pages. This technology provides many features, such as writing to disk or execution of commands at the client (i.e. on the host where the Web page is opened). This technology provides a wide range of features, such as saving to disk and running commands at the client (i.e. at the computer where the Web page is opened). Using *ActiveX*, virus and worms can for example modify telephone number of the dial-up.

ActiveX is supported only by *Microsoft Internet Explorer* in *Microsoft Windows* operating systems.

Cluster

A group of two or more workstations representing one virtual host (server). Requests to the virtual server are distributed among individual hosts in the cluster, in accordance with a defined algorithm. Clusters empower performance and increase reliability (in case of dropout of one computer in the cluster, the virtual server keeps running).

Connections

Bidirectional communication channel between two hosts. See also *TCP*.

Default gateway

A network device or a host where so called default path is located (the path to the Internet). To the address of the default gateway such packets are sent that include destination addresses which do not belong to any network connected directly to the host and to any network which is recorded in the system routing table.

In the system routing table, the default gateway is shown as a path to the destination network *0.0.0.0* with the subnet mask *0.0.0.0*.

Note: Although in *Windows* the default gateway is configured in settings of the network interface, it is used for the entire operating system.

DHCP

DHCP (*Dynamic Host Configuration Protocol*) Serves automatic IP configuration of computers in the network. IP addresses are assigned from a scope. Besides IP addresses, other parameters can be associated with client hosts, such as the default gateway address, DNS server address, local domain name, etc.

DNS

DNS (*Domain Name System*) A worldwide distributed database of Internet hostnames and their associated IP address. Computers use Domain Name Servers to resolve host names to IP addresses. Names are sorted in hierarchized domains.

Firewall

Software or hardware device that protects a computer or computer network against attacks from external sources (typically from the Internet).
In this guide, the word *firewall* represents the *WinRoute* host.

FTP

File Transfer Protocol. The FTP protocol uses two types of TCP connection: control and data. The control connection is always established by a client. Two FTP modes are distinguished according to a method how connection is established:

- *active mode* — data connection is established from the server to a client (to the port specified by the client). This mode is suitable for cases where the firewall is at the server's side, however, it is not supported by some clients (e.g. by web browsers).
- *passive mode* — data connection is established also by the client (to the port required by the server). This mode is suitable for cases where the firewall is at the client's side. It should be supported by any FTP client.

Note: WinRoute includes special support (protocol inspector) for FTP protocol. Therefore, both FTP modes can be used on LAN hosts.

Gateway

Network device or a computer connecting two different subnets.

Greylisting

A method of protection of *SMTP* servers from spam. If an email message sent by an unknown sender is delivered to the server, the server rejects it for the first time (so called temporary delivery error). Legitimate senders attempt resend the message after some time. SMTP server lets the message in and considers the sender as trustworthy since then, not blocking their messages any longer. Most spam senders try to send as great volume in as short time as possible and stay anonymous. Therefore, they usually do not repeat sending the message and focus on another SMTP server.
More information (in English) can be found for example at Wikipedia.

IMAP

Internet Message Access Protocol (IMAP) enables clients to manage messages stored on a mail server without downloading them to a local computer. This architecture allows the user to access his/her mail from multiple locations (messages downloaded to a local host disk would not be available from other locations).

IP address

IP address is a unique 32-bit number used to identify the host in the Internet. It is specified by numbers of the decimal system (0–255) separated by dots (e.g. 195.129.33.1). Each packet contains information about where it was sent from (source IP address) and to which address it is to be delivered (destination IP address).

IPSec

IPsec (*IP Security Protocol*) is an extended IP protocol which enables secure data transfer. It provides services similar to SSL/TLS, however, these services are provided on a network layer. IPSec can be used for creation of encrypted tunnels between networks (VPN) — so called tunnel mode, or for encryption of traffic between two hosts— so called transport mode.

Kerberos

Kerberos is a system used for secure user authentication in network environments. It was developed at the MIT university and it is a standard protocol used for user authentication under Windows 2000/2003. Users connect to central servers (Key Distribution Center — KDC) and the servers send them encrypted keys (so called tickets) for connection to other servers within the network. In case of the Windows 2000/2003 domains, function of *KDC* is provided by the particular domain server.

LDAP

LDAP (Lightweight Directory Access Protocol) is an Internet protocol used to access directory services. Information about user accounts and user rights, about hosts included in the network, etc. are stored in the directories.

NAT

NAT (*Network Address Translation*) stands for substitution of IP addresses in packets passing through the firewall:

- source address translation (*Source NAT, SNAT*) — in packets going from local networks to the Internet source (private) IP addresses are substituted with the external (public) firewall address. Each packet sent from the local network is recorded in the NAT table. If any packet incoming from the Internet matches with a record included in this table, its destination IP address will be substituted by the IP address of the appropriate host within the local network and the packet will be redirected to this host. Packets that do not match with any record in the NAT table will be dropped.
- destination address translation (*Destination NAT, DNAT*, it is also called port mapping) — is used to enable services in the local network from the Internet. If any packet incoming from the Internet meets certain requirements, its IP address will be substituted by the IP address of the local host where the service is running and the packet is sent to this host.

The *NAT* technology enables connection from local networks to the Internet using a single IP address. All hosts within the local network can access the Internet directly as if they were on a public network (certain limitations are applied). Services running on local hosts can be mapped to the public IP address.

Network adapter

The equipment that connects hosts to a traffic medium. It can be represented by an Ethernet adapter, TokenRing adapter, by a modem, etc. Network adapters are used by hosts to send and receive packets. They are also referred to throughout this document as a network interface.

P2P network

Peer-to-Peer (*P2P*) networks are world-wide distributed systems, where each node can represent both a client and a server. These networks are used for sharing of big volumes of data (this sharing is mostly illegal). *DirectConnect* and *Kazaa* are the most popular ones.

Packet

Basic data unit transmitted via computer networks. Packets consist of a header which include essential data (i.e. source and destination IP address, protocol type, etc.) and of the data body,. Data transmitted via networks is divided into small segments, or packets. If an error is detected in any packet or a packet is lost, it is not necessary to repeat the entire transmission process, only the particular packet will be re-sent.

POP3

Post Office Protocol is a protocol that enables users to download messages from a server to their local computer. It is suitable for clients who don't have a permanent connection to the Internet.

Port

16-bit number (`1–65535`) used by TCP and UDP for application (services) identification on a given computer. More than one application can be run at a host simultaneously (e.g. WWW server, mail client, FTP client, etc.). Each application is identified by a port number. Ports `1–1023` are reserved and used by well known services (e.g. `80` = WWW). Ports above `1023` can be freely used by any application.

PPTP

Microsoft's proprietary protocol used for design of virtual private networks (see chapters concerning *VPN*).

Private IP addresses

Local networks which do not belong to the Internet (private networks) use reserved ranges of IP addresses (private addresses). These addresses cannot be used in

the Internet. This implies that IP ranges for local networks cannot collide with IP addresses used in the Internet.

The following IP ranges are reserved for private networks:

- `10.0.0.0/255.0.0.0`
- `172.16.0.0/255.240.0.0`
- `192.168.0.0/255.255.0.0`

Protocol inspector

WinRoute's plug-in (partial program), which is able to monitor communication using application protocols (e.g. HTTP, FTP, MMS, etc.). Protocol inspection is used to check proper syntax of corresponding protocols (mistakes might indicate an intrusion attempt), to ensure its proper functionality while passing through the firewall (e.g. FTP in the active mode, when data connection to a client is established by a server) and to filter traffic by the corresponding protocol (e.g. limited access to Web pages classified by URLs, anti-virus check of downloaded objects, etc.).

Unless traffic rules are set to follow a different policy, each protocol inspector is automatically applied to all connections of the relevant protocol that are processed through *WinRoute*.

Proxy server

Older, but still wide-spread method of Internet connection sharing. Proxy servers connect clients and destination servers.

A proxy server works as an application and it is adapted for several particular application protocols (i.e. HTTP, FTP, Gopher, etc.). It requires also support in the corresponding client application (e.g. web browser). Compared to NAT, the range of featured offered is not so wide.

Routing table

The information used by routers when making packet forwarding decisions. Packets are routed according to the packet's destination IP address. The routing table can be viewed in Windows operating systems using the `route print` command.

Script

A code that is run on the Web page by a client (Web browser). Scripts are used for generating of dynamic elements on Web pages. However, they can be misused for ads, exploiting of user information, etc. Modern Web browsers usually support several script languages, such as *JavaScript* and *Visual Basic Script (VBScript)*.

SMTP

Simple Mail Transfer Protocol is used for sending email between mail servers. The SMTP envelope identifies the sender/recipient of an email.

Spam

Undesirable email message, usually containing advertisments.

Spoofing

Spoofing means using false IP addresses in packets. This method is used by attackers to make recipients assume that the packet is coming from a trustworthy IP address.

SSL

SSL is a protocol used to secure and encrypt network communication. SSL was originally designed by *Netscape* in order to ensure secure transfer of Web pages over HTTP protocol. Nowadays, it is used by most standard Internet protocols (SMTP, POP3, IMAP, LDAP, etc.).

At the beginning of communication, an encryption key is requested and transferred using asymmetrical encryption. This key is then used to encrypt (symmetrically) the data.

Subnet mask

Subnet mask divides an IP address in two parts: network mask and an address of a host in the network. Mask have the same form as IP addresses (i.e. `255.255.255.0`), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. Number one in a subnet mask represents a bit of the network address and zero stands for a host's address bit. All hosts within a particular subnet must have identical subnet mask and network part of IP address.

TCP

Transmission Control Protocol is a transmission protocol which ensures reliable and sequentional data delivery. It establishes so called virtual connections and provides tools for error correction and data stream control. It is used by most of applications protocols which require reliable transmission of all data, such as *HTTP*, *FTP*, *SMTP*, *IMAP*, etc.

TCP protocol uses the following special control information — so called *flags*:

- *SYN* (Synchronize) — connection initiation (first packet in each connection)
- *ACK* (Acknowledgement) — acknowledgement of received data
- *RST* (Reset) — request on termination of a current connection and on initiation of a new one
- *URG* (Urgent) — urgent packet
- *PSH* (Push) — request on immediate transmission of the data to upper TCP/IP layers
- *FIN* (Finalize) — connection finalization

TCP/IP

Name used for all traffic protocols used in the Internet (i.e. for IP, ICMP, TCP, UDP, etc.). *TCP/IP* does not stand for any particular protocol!

TLS

Transport Layer Security. New version of SSL protocol. This version is approved by the IETF and it is accepted by all the top IT companies (i.e. Microsoft Corporation).

UDP

User Datagram Protokol is a transmission protocol which transfers data through individual messages (so called datagrams). It does not establish new connections nor it provides reliable and sequentional data delivery, nor it enables error correction or data stream control. It is used for transfer of small-sized data (i.e. DNS queries) or for transmissions where speed is preferred from reliability (i.e. realtime audio and video files transmission).

VPN

Virtual Private Network, VPN represents secure interconnection of private networks (i.e. of individual offices of an organization) via the Internet. Traffic between both networks (so called tunnel) is encrypted. This protects networks from tapping. VPN incorporates special tunneling protocols, such as *Microsoft's IPSec* and *PPTP* (*Point-to-Point Tunnelling Protocol*).

WinRoute contains a proprietary VPN implemetation called *Kerio VPN*.

Index

A

Active Directory *189*, *196*
  automatic import of accounts *197*
  domain mapping *199*
  import of user accounts *198*
  multiple domains mapping *202*
administration *27*
  remote *25*, *209*
Administration Console *27*
  views setup *30*
alerts *246*
  overview *249*
  settings *246*
  templates *248*
anti-spoofing *217*
antivirus check *14*, *160*
  conditions *160*
  external antivirus *164*
  file size limits *164*
  HTTP and FTP *166*
  McAfee *162*
  protocols *164*
  rules for file scanning *168*
  settings *162*
  SMTP and POP3 *170*

B

bandwidth limiter *113*
  configuration *114*
  detection principle *118*
beta version *381*
BOOTP *75*

C

certificate
  SSL-VPN *356*
  VPN server *301*
  Web Interface *128*
Clientless SSL-VPN
  antivirus check *359*
  bookmarks *359*
  certificate *356*, *355*
  configuration *355*
  deployment *357*
  port *356*
  traffic rule *356*
  user right *191*, *207*
cluster *375*
configuration files *361*
  manipulation *363*
  recovery *363*
conflict
  port *13*
  software *13*
  system services *19*
connection failover
  configuration *57*, *56*

D

default gateway
  configuration detection *360*
DHCP
  default options *68*, *66*
  IP scopes *67*
  lease reservations *72*
  leases *73*
DirecWay *87*

DNS
DNS Forwarder 60
forwarding rules 62
hosts file 64, 65
local domain 65

F

FTP
filtering rules 155, 137, 179, 372

G

groups
IP address 173
of forbidden words 153
URL 180
user groups 183, 189, 204

H

H.323 180
HTTP
cache 80
content filtering 146
content rating 147
filtering by words 151, 137
logging of requests 145
proxy server 76
URL Rules 138

I

import
user accounts 197, 198
installation 15
interface throughput charts
anti-spoofing 217
demand dial 54, 225
Dial-In 51
dial-up 51, 49
IPSec
client 219
configuration 219, 218
server 221
ISS OrangeWeb Filter
deployment 149, 147
parameters configuration 148
website categories 150

K

Kerberos 189
Kerio Administration Console 21, 27
views setup 30

L

language
Administration Console 27
of alerts 249
Web Interface 130
license
expiration 44
information 34, 32
license key 32
license types 32
number of users 33
optional components 32
user counter 46
license key 44
localizations
Administration Console 27
of alerts 249
Web Interface 130
log
alert 283
config 284
connection 285
debug 286
dial 286
error 289
filter 290
http 291, 275
security 293
settings 275
sslvpn 295
warning 295

web *296*

M

multihoming *109*

N

NAT *92*, *103*, *106*
NLB
  configuration *375*, *375*
NT domain
  import of user accounts *198*, *196*
NTLM
  configuration of web browsers *368*
  deployment *365*, *123*
  WinRoute configuration *366*

P

P2P Eliminator *213*
Peer-to-Peer (P2P) networks
  allow *191*, *208*
  deny *213*
  detection *238*, *213*
  ports *215*
  speed limit *213*
port
  SSL-VPN *356*
port mapping *90*, *104*, *107*
product registration *32*
protocol inspector *105*, *178*, *179*
  retirement *369*
proxy server
  parent *79*, *76*, *372*

Q

Quick Setup *8*
quota
  settings *258*

R

ranges
  time *174*, *175*
RAS *51*, *75*
registration
  at the Kerio website *44*
  of purchased product *39*
  trial version *36*
relay SMTP server *231*
routing table *222*
  static routes *223*

S

services *100*, *177*
SIP *180*
SSL-VPN
  antivirus check *359*
  bookmarks *359*
  certificate *356*
  configuration *355*
  deployment *357*
  port *356*, *355*
  traffic rule *356*
  user right *191*, *207*
StaR
  accounting period *263*
  conditions for statistics *258*
  enable/disable gathering of statistic data *257*
  overall view *265*, *269*
  overview *261*
  settings *258*, *257*
  top requested web categories *272*
  top visited websites *271*
  volume of transferred data *270*
statistics
  accounting period *263*
  conditions for statistics *258*
  interface throughput charts *251*
  in the Web interface *257*
  Kerio StaR *257*
  monitoring *257*
  overall view *265*, *269*
  overview *261*

settings *258*, *251*
top requested web categories *272*
top visited websites *271*
user groups *254*
volume of transferred data *270*
status information
active hosts *234*
connections *242*, *234*
subscription
expiration *44*
Syslog *277*

T

technical support
contacts *382*, *380*
traffic policy
created by wizard *93*
default rule *95*
definition *96*
exceptions *111*
Internet access limiting *109*, *86*
wizard *86*
transparent proxy *80*
Trial ID *39*
TTL *80*, *84*

U

uninstallation *23*
update
antivirus *162*
WinRoute *210*
upgrade
automatic update *210*, *16*, *22*
UPnP
settings *230*
system services *19*
user accounts
automatic import *197*
definition *184*
domain mapping *199*
local *185*, *186*
mapped *186*
templates *185*, *188*, *183*
user authentication
authentication methods *189*
automatic login *195*
configuration *122*
in Active Directory *196*
in NT domain *196*
login page *130*, *121*

V

VPN
client *191*, *207*, *304*
configuration example *313*
IPSec *218*
Kerio Clientless SSL-VPN *355*
Kerio VPN *298*
routing *311*
server *51*, *299*
SSL certificate *301*
tunnel *305*, *298*
VPN client
DNS *302*
routing *302*
static IP address *195*, *304*
VPN tunnel
configuration *305*
DNS *308*
routing *308*
traffic policy *310*, *305*

W

Web interface
automatic configuration *79*
configuration script *79*
Web Interface
language preferences *130*
login page *130*
parameters configuration *125*
ports *127*
SSL certificate *128*

user preferences *134*
user statistics *133*, *125*
Windows
Internet Connection Sharing *19*
security center *20*
Windows Firewall *19*
WinRoute Engine Monitor *20*, *21*
WinRoute Firewall Engine *20*
WinRoute Pro *24*
wizard
configuration *24*
traffic rules *86*